COUNCIL OF THE EUROPEAN UNION

Brussels, 17 November 2010

15458/10

COPEN 238
JURINFO 51
EJUSTICE 106

NOTE

from:	General Secretariat of the Council
to:	Delegations
Subject:	ECRIS Technical Specifications - Inception Report

On 6th October 2010 the Presidency launched written procedure for the adoption of the Inception Report, revised further to the observations submitted by the delegations and examined during the discussions at the Working Party on Cooperation in Criminal Matters which met on 2 September 2010. This procedure ended on 15 October 2010 COB.

No objections have been received from any Member State in respect of the modifications introduced into the text of Inception Report, as set out in 14558/10 COPEN 204 EJUSTICE 85 JURINFO 43.

Accordingly, the modified Inception Report is deemed adopted and will be the basis for further work on the implementation of ECRIS.

Delegations will find in the Annex the revised text of the Inception Report on the implementation of ECRIS, as agreed upon following the above mentioned procedure.

ANNEX

European Commission – DG Justice

iLICONN Consortium (Bilbomatica – Intrasoft – Unisys)

ECRIS Technical Specifications

Inception Report

Document Information

AUTHOR	iLICONN – Intrasoft International S.A.
OWNER	European Commission – DG Justice
ISSUE DATE	22/10/2010
VERSION	1.02
APPROVAL STATUS	Adopted

Authors

NAME	ACRONYM	ORGANISATION	ROLE
Margaret TUITE	MTU	European Commission – DG Justice	Responsible Reviewer
Jaime LOPEZ-LOOSVELT	JLO	European Commission – DG Justice	Manager Reviewer
Urszula-Aurelia KARKOWSKA	UKA	European Commission – DG Justice	Reviewer
Nicholas YIALELIS	NYI	iLICONN – Intrasoft International S.A.	Manager Reviewer
Ludovic COLACINO DIAS	LCO	iLICONN – Intrasoft International S.A.	Main Author
Panos ATHANASIOU	PAT	iLICONN – Intrasoft International S.A.	Contributor
Daniel COMAN	DCO	iLICONN – Intrasoft International S.A.	Contributor
Ann Mennens	AME	iLICONN – Unisys Belgium	Reviewer
Marc Lombaerts	MLO	iLICONN – Unisys Belgium	Reviewer

Document History

VERSION	DATE	AUTHOR	DESCRIPTION
0.01	20/08/2010	LCO	First draft
0.02	29/08/2010	LCO	Revision of all sections, consolidation of all comments received from all reviewers and contributors
1.00	04/10/2010	LCO	Update of all sections according to feedback on author's position and outcome of COPEN meeting 27-Sep-2010 Final version (for adoption by COPEN)
1.01	05/10/2010	LCO	Update of final version after remarks from Commission
1.02	22/10/2010	LCO	Text of version 1.01, adopted in Council by COPEN Working Party on 20-Oct-2010

TABLE OF CONTENTS

DOCUMENT

Purpose

This document is the first formal product of the *ECRIS Technical Specifications* project, for the European Commission – DG Justice and produced by the iLICONN Consortium.

The main purpose of this document is to set a common background, common understanding and common basis of work for the experts of the 27 Member States of the European Union, the European Commission and iLICONN in view of producing and agreeing on a set of technical specifications for implementing the ECRIS system described in the Council Framework Decision 2009/315/JHA of 26 February 2009 and in the Council Decision 2009/316/JHA of 06 April 2009.

More specifically, the *ECRIS Technical Specifications* project has the following objectives:

1. The adoption of technical specifications for the exchange of information extracted from criminal records, including security requirements, in particular the common set of protocols.
2. The establishment of logging systems and procedures making it possible to monitor the functioning of ECRIS and the establishment of non-personal statistics relating to the exchange through ECRIS of information extracted from criminal records.
3. The establishment of procedures verifying the conformity of the national software applications with the technical specifications.

This document assumes that the readers have a good and detailed knowledge and understanding of the ECRIS legal basis.

Scope

This document provides the background information on which the *ECRIS Technical Specifications* project is further based. As such, it focuses principally on the elaboration of a set of IT-technical specifications for the ECRIS data exchange system. Therefore the term “project” refers only and specifically to the *ECRIS Technical Specifications* project throughout this document.

This document provides:

- a detailed description of the project’s legal framework and context
- a detailed description of the project’s calendar and of the working methods to be applied
- the list of assumptions and constraints on which the project is based

- a detailed description of the scope of the project; in particular it determines the functionality and behaviour to be implemented in the ECRIS software applications and thus be supported by the ECRIS technical specifications; it also outlines the parts of the data exchange processes that are to be handled within each Member States administrations and that are not directly part of the ECRIS software applications
- a detailed list of subjects that have been identified as requiring additional study, in collaboration with the criminal records experts of the EU Member States
- a proposal for the global roadmap to be followed in view of implementing successfully the ECRIS legal basis; it describes a roadmap that would allow the EU Member States to implement ECRIS and the criminal records data exchanges to be operational by April 2012
- a list of risks that have been identified so far and which are potential threats for the implementation of the ECRIS decisions

This document does not provide more information than what is stated above, and in particular it does not include:

- proposals for the technical architecture of the ECRIS data exchange software systems
- detailed legal, functional and/or IT-technical studies
- IT-security analyses
- the ECRIS technical specifications
- business cases, use cases, test scenarios and test cases

References

The following documents have been used as input for the elaboration of this "Inception Report":

[1] ECRIS Legal Basis – Council Framework Decision 2009/315/JHA
Council of the European Union (2009), Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States (OJ L 93/23 of 07.04.2009)

[2] ECRIS Legal Basis – Council Decision 2009/316/JHA
Council of the European Union (2009), Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA (OJ L 93/33 of 07.04.09)

[3] Council of the European Union (2010), letter 11286/10 of 05 July 2010 from the Presidency to the Member States delegations

[4] European Commission – DG Justice, Freedom and Security (2006): Final report on the study of the "Review of National Criminal Records Systems in the European Union, Bulgaria and Romania with the view of the Development of a Common Format for the Exchange of Information on Criminal Records" (July, 2006)

[5] Network of Judicial Registers (NJR) – Functional Concept – version 1.4a (approved) of 02 August 2010

[6] Network of Judicial Registers (NJR) – Technical References – version 1.3a (approved) of 13 March 2008

[7] Network of Judicial Registers (NJR) – Technical References – version 1.4 (draft) of 23 November 2009

[8] Network of Judicial Registers (NJR) – XML Listings – version 1.4 (final) of 01 July 2009

[9] NJR WSDL and XML Files v1.4.2 of 21 January 2009 (final) "CommonTables_and_XML_rel1-4-2_20090121.zip" file containing:

- RegisterService-1.4.2.wsdl (version 1.4.2)
- common.xsd (version 1.4 of 18 December 2008)
- CommonTables-1.3.xsd (version 1.3)
- CommonTables-1.4.2.xml (version 1.4.2)
- error.xsd (version 1.4 of 02 November 2005)
- information.xsd (version 1.4 of 02 November 2005)
- notification.xsd (version 1.4 of 22 November 2005)
- receipt.xsd (version 1.4 of 02 November 2005)
- request.xsd (version 1.4 of 02 November 2005)

[10] NJR WSDL and XML Files v1.5 (draft)

- RegisterService-1.5.wsdl (draft version 1.5 of 11 August 2010)
- common.xsd (draft version 1.5 of 10 June 2010)
- CommonTables-1.5.xsd (draft version 1.5)
- CommonTables-1.5.xml (draft version 1.5.0)
- error.xsd (draft version 1.5 of 10 July 2010)
- information.xsd (draft version 1.5 of 10 July 2010)
- notification.xsd (draft version 1.5 of 10 July 2010)
- receipt.xsd (draft version 1.5 of 10 July 2010)
- request.xsd (draft version 1.5 of 10 July 2010)

[11] Network of Judicial Registers (NJR) – Common Statistics 2.1 Guidelines – version 1.1 of 06 July 2010

[12] Network of Judicial Registers (NJR) – Tests for release 1.4.2 – version 1.0 (draft) of 02 July 2009

[13] European Commission – DG Enterprise (2004): IDA Architecture Guidelines for Trans-European Telematics Networks for Administrations, version 7.1 of 13 February 2004 (and annexes)

[14] Supporting documents of the NJR Technical Workshop in Lisbon, 16-17 June 2010:

- PowerPoint presentation: Change Management (Oscar Caraballo, Andreas Rudloff)
- PowerPoint presentation: NJR goes ECRIS (Oscar Caraballo, Andreas Rudloff)

[15] Supporting document of the NJR Technical Workshop in Bratislava, 03-04 June 2009:

- PowerPoint presentation: NJR meets ECRIS – Common Reference Tables (Stefanie Lau)

About this Document

Elaboration of this Document

This "Inception Report" has been drafted by the iLICONN staff based on the following input:

§ The documents listed in the references above

§ Preliminary on-site visits of the following Member States' central authorities:

- 19-Jul-2010 / 30-Jul-2010: Belgium – Service Public Fédéral Justice – Service Casier Judiciaire Central
- 26-Jul-2010 : France – Ministère de la Justice – Casier Judiciaire National
- 29-Jul-2010 : Germany – Bundesamt für Justiz – Bundeszentralregister
- 05-Aug-2010 : United Kingdom – Association of Chief Police Officers (ACPO) – ACPO Criminal Records Office (ACRO)
- 09-Aug-2010 : Spain – Ministerio de Justicia – Registro central de penados y rebeldes

§ The answers provided by the following Member States' central authorities to the questions defined in the *Inception Phase Questionnaire* document that has been sent out by the European Commission to all Member States' contact points on the 04th of August 2010 (listed in alphabetical order):

Austria (AT), Belgium (BE), the Czech Republic (CZ), Estonia (EE), Finland (FI), France (FR), Germany (DE), Hungary (HU), Lithuania (LT), Luxembourg (LU), the

Netherlands (NL), Poland (PL), Portugal (PT), Romania (RO), Slovakia (SK), Slovenia (SI), Spain (ES), Sweden (SE), the United Kingdom (UK)

- Direct contacts and meetings with various experts (various experts from the European Commission, experts from the contractor currently developing the *NJR Reference Implementation* software but also other experts that have been involved in various studies and similar projects in the field of justice and cooperation in criminal matters).
- The 181 comments issued by the Member States on the previous version of this document by the 08th of September 2010.
- The author's position on these comments, provided in the "Inception Report – Inspection Sheet" spread-sheet (v1.2 of 16 September 2010) and the "Inception Report – Author's Position" document (v0.01 of 16 September 2010)
- The agreements and conclusions reached by the 27 Member States during the COPEN meeting of the 27th of September 2010.

Understanding this Document

This "Inception Report" comes with a "Glossary" document that provides definitions for the specific terms that are used throughout the *ECRIS Technical Specifications* project.

By convention, all words marked in italic in this document can be looked up in the "Glossary" document. The bold font and underlines are used for emphasising a specific term or part of a sentence.

In case of doubts about the exact meaning of a term, please consult first the "Glossary".

Should you still have any doubts about the meaning of a specific sentence or paragraph, please do not hesitate to take direct contact with the following persons by telephone or via e-mail, at your best convenience:

Organisation: European Commission – DG Justice – Criminal Law

Name: Jaime LOPEZ-LOOSVELT

E-mail: JUST-CRIMINAL-RECORD@ec.europa.eu

Telephone: +32 (0)2.298.41.54

Organisation: iLICONN Consortium – Intrasoft International S.A.

Name: Ludovic COLACINO DIAS

E-mail: ECRIS-Specs-PM.iLICONN@intrasoft-intl.com

Mobile: +32 (0)498.30.25.55

Providing Comments

As described later in this document, all major deliverables produced by the iLICONN Consortium are undergoing a "Review Cycle" during which all EU Member States experts are invited to provide comments.

Since the iLICONN staff needs to collect, compare and analyse the feedback from 27 Member States on the same document – thus potentially a large number of comments – it uses a tool that allows easily extracting the comments from MS Word documents.

Therefore, for commenting this document, please apply the following guidelines:

- All comments are to be written in plain English. Comments provided in other languages cannot, unfortunately, be taken into account.
- The comments must be specific to and must relate to the text (sentence and/or paragraph) being revised.
- Please use simple wording and be as specific, concise and clear as possible in order to avoid ambiguities.
- When referring to specific terms, acronyms, abbreviations that are common in your daily jargon but that are not defined in the *Glossary* document, please define them first.
- Write your comments directly in this MS Word document, by proceeding as follows:
  - First select a word, a part of a sentence or a paragraph (this can be done for example by double-clicking on a word or by dragging your mouse over parts of the text while keeping the left mouse-button pressed).
    Attention:

    Please note that a **minimum of 4 characters** must be selected in order for our commenting tool to grab the comment. Furthermore, comments on diagrams and embedded pictures are also not taken into account. In such cases, please select the caption text underneath the diagram or image.
  - Once a word, part of a sentence or paragraph has been selected, insert an MS Word comment in which you can type your remarks.
    An MS Word comment is typically displayed as a red balloon in the right margin of the document and usually starts with the abbreviation of your name and the timestamp at which the comment is being written. Depending on your version of MS Word, use the following steps for inserting a comment:

MS Word 2007 and MS Word 2010:

4. Select the text you would like to comment upon
5. Open the **Review** ribbon, select **New Comment** in the **Comments** section
6. In the balloon that appears in the right margin, type your comment
7. Click anywhere in the document to continue editing the document

MS Word 2003:

1. Select the text you would like to comment upon
2. From the **Insert** menu, select **Comment** (or click on the **New Comment** button on the **Reviewing** toolbar)
3. In the balloon that appears in the right margin, type your comment
4. Click anywhere in the document to continue editing the document

The text will have coloured lines surrounding it, and a dotted coloured line will connect it to the comment. To delete a comment, simply right click on the balloon and select **Delete Comment**.

§ Please do not use the MS Word "track changes" tool and do not write your comments as plain text in the MS Word file.

§ In case that you want to provide general comments or remarks that are not specific to a part of the text of this document, please provide them into a separate document and/or e-mail.

§ In case that you need to translate this document to another language, and then translate back your comments to English, please make sure that your comments are provided in the form described above and that they have not been altered or moved to another section of the text during the translation process.

ECRIS TECHNICAL SPECIFICATIONS: INTRODUCTION

General

From its very beginning, European integration has been firmly rooted in a shared commitment to freedom based on human rights, democratic institutions and the rule of law. These common values have proved necessary for securing peace and developing prosperity in the European Union. They will also serve as a cornerstone for continuing enlarging the Union.

One of the fundamental objectives of the European Union, as repeated by the Treaty of Lisbon that entered into force on 01 December 2009, is to offer its citizens an area of freedom, security and justice without internal borders.

In a 21st century European Union, the free movement of persons, besides acting as one of the main prerequisites for an economic, social and political development and integration of any of its 27 Member States, also raises important issues. The more and more trans-national nature of criminality, with a particular emphasis on terrorism and organised crime, identifies new challenges for the Member States' judicial authorities and request appropriate answers.

Since the early conclusions of the Tampere European Council of October 1999[1], the implementation of the principle of mutual recognition in criminal matters has become a priority in the EU's efforts to strengthen the security in the area of freedom, security and justice. Improving the quality of information exchange on convictions was set as an objective in the European Council Declaration on Combating Terrorism of March 2004[2], further reiterated in the Hague Programme, and adopted by the European Council on November 2004[3].

[1] EUROPEAN COUNCIL (1999) – Tampere Presidency Conclusions (SN 200/1/99 REV 1)
[2] EUROPEAN COUNCIL (2004) – Declaration on Combating Terrorism (Brussels, 25/03/2004)
[3] EUROPEAN COUNCIL (2004) – The Hague Programme: strengthening freedom, security and justice in the European Union (OJ C 53/11 of 03/03/2005)

Awaiting the outcome of the Council meeting (Justice and Home Affairs) on 14 April 2005, following the publication in January 2005 of the White Paper on exchanges of information on convictions and the effect of such convictions in the European Union and the subsequent general discussion thereof, the partners of the *Network of Judicial Registers (NJR)* project have agreed to exchange such information via electronic means and effectively started these exchanges on 31 March 2006. The normative framework governing the NJR activities at European level consists of Articles 13 and 22 of the European Convention on Mutual Assistance, adopted by the Council of Europe in 1959[4].

On 21 November 2005 the Council adopted a first proposal from the Commission for a Council Decision on the exchange of information extracted from criminal records[5], the purpose of which was to improve the system of the 1959 Convention in the short term. In June 2007 the Council reached a political agreement on the Framework Decision aiming to ensure that a Member State is able to respond properly and fully to requests made to it regarding the criminal records of its nationals, and to lay down the basis for a computerised conviction-information exchange system. Further discussions as well as experience gained from the NJR project resulted in the Commission's proposal for a Council Decision on the establishment of the European Criminal Records Information System (ECRIS)[6].

[4] COUNCIL OF EUROPE (1959) – European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 20/04/1959)

[5] COUNCIL OF THE EUROPEAN UNION (2005) – Council decision 2005/876/JHA of 21 November 2005 on the exchange of information extracted from the Criminal Records (OJ L 322 of 09/12/2005)

[6] EUROPEAN COMMISSION (2008) – Proposal for "A Council Decision on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2008/XX/JHA" (COM(2008) 332 final)

On 26 February 2009, the Council Framework Decision[7] was adopted establishing a mechanism for improving the circulation of information on convictions in the European Union.

This Framework Decision replaced Article 22 of the Convention on Mutual Assistance in Criminal Matters regarding notifications between EU Member States. The Decision has also provided for the establishment of a computerised exchange of information on convictions between Member States (ECRIS), provided for in the ECRIS Decision[8].

ECRIS Legal Basis

The ECRIS legal basis is constituted of the Council Framework Decision 2009/315/JHA of 26 February 2009 and of the Council Decision 2009/316/JHA of 06 April 2009. It sets the legal ground for the implementation of the ECRIS system for the exchanges of criminal records data between the EU Member States.

Summary

This chapter summarises the main elements of the legal basis to be taken into account for the definition of the *ECRIS Technical Specifications*.

Please note that the following text does not replace or supplement in any way the *ECRIS Legal Basis*. It does not constitute an exhaustive summary of the *ECRIS Legal Basis* either; it rather focuses on the parts that are of interest to define the ECRIS software system and its expected behaviour. The aim of the following is to outline the major aspects of this legal basis to keep in mind when reading through the rest of this document and during the elaboration of the *ECRIS Technical Specifications*.

---

[7] COUNCIL OF THE EUROPEAN UNION (2009) – Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States (OJ L 93/23 of 07/04/2009)

[8] COUNCIL OF THE EUROPEAN UNION (2009) - Council Decision of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA (OJ L 93/33 of 07.04.09)

General

ECRIS stands for "European Criminal Records Information System". It is defined as a decentralised information technology system composed of (1) a piece of interconnection software, built in compliance with a common set of protocols, and (2) of the sTESTA network as the common communication infrastructure.

The purpose of ECRIS is to enable the effective and systematic exchange between the competent authorities of the Member States of information extracted from criminal records in such a way that would guarantee its common understanding and the efficiency of such exchange.

The criminal records data is to be stored solely in databases operated by the Member States and there shall be no direct online access to criminal records databases between Member States. In particular, the interconnection software and databases storing, sending and receiving information extracted from criminal records shall operate under the responsibility of the Member State concerned. The sTESTA network shall be operated under the responsibility of the European Commission.

Each Member State shall designate one or more central authorities responsible for the transmission of information on criminal records and using ECRIS.

Exchange of Information

Notifications of convictions and subsequent changes

Each time a *conviction* is entered in the criminal records *register* of a *convicting Member State* and concerns a person being a national of one or more other Member States, the *convicting Member State* must notify[9] these other Member States of the *conviction* as soon as possible. In addition, information on subsequent alterations or removal of information contained in the criminal records of the *convicting Member State* must be immediately transmitted[10] to the Member States of nationality of the convicted person. Any such alterations or deletions of information transmitted by the *convicting Member State* shall entail identical alteration or deletion[11] by the Member State of the person's nationality regarding the information that has been stored for the purpose of the retransmission to requesting Member States.

[9] Council Framework Decision 2009/315/JHA – Article 4, paragraph 2

[10] Council Framework Decision 2009/315/JHA – Article 4, paragraph 3

11 Council Framework Decision 2009/315/JHA – Article 5, paragraph 2

When notifying the central authority of the Member State of the person's nationality, the *convicting Member State* may also inform that the conviction information cannot be retransmitted to other Member States for purposes other than criminal proceedings[12].

Requests for information on criminal record data

The central authority of a Member State may, according to its national law, issue a request to the central authority of another Member State for information and related data to be extracted from the criminal record of a person (who does not necessarily have the nationality of the requested Member State). The legal basis foresees the possibility to issue such requests for purposes of criminal proceedings against a person but also for any other purposes (such as for example administrative purposes, employment vetting, an individual's request for obtaining his or her own criminal record, etc.).

Replies to requests for information on criminal record data

When a request is issued by a Member State for **purposes of criminal proceedings**[13] to the Member State of the person's nationality, the latter's central authority must transmit to the requesting Member State convictions that have been stored in its criminal records register, in particular including:

(1) the convictions handed down in the Member State of the person's nationality,
(2) **any** convictions handed down in another Member State which have been notified to the Member State of the person's nationality and
(3) **any** convictions handed down in third countries which have been notified to the Member State of the person's nationality and stored in the criminal records register.

For requests that are issued **for purposes other than criminal proceedings**[14], the requested Member State's central authority shall provide the convictions entered in its criminal records register in accordance with its national law. In this scenario, the convictions that have been handed down in another Member State and for which the *convicting Member State* informed the Member State of the person's nationality that they may not be retransmitted for purposes other than criminal proceedings, may not be included in the response to the requesting Member State. In this particular case, the requested Member State shall inform the requesting Member State which other convicting Member State(s) to contact directly in order to obtain information on convictions of the person in question.

12 Council Framework Decision 2009/315/JHA – Article 7, paragraph 2(3)

13 Council Framework Decision 2009/315/JHA – Article 7, paragraph 1

14 Council Framework Decision 2009/315/JHA – Article 7, paragraph 2

Deadlines for replies to requests for information on criminal record data

Independently of the purpose of the request, the requested Member State's central authority must provide its response as soon as possible, and at the latest within a period of **10 working**[15] **days** from the date the request was received, to the requesting Member State's central authority. In the case where further information is required to identify the person involved in the request, the requested Member State shall immediately consult the requestor and then provide the reply within **10 working days** from the date when the additional information was received[16].

In the specific case where a request to another Member State is issued by a central authority of a Member State on behalf of a person who asks for his own criminal record, then the reply must be provided within **20 working days**[17] from the date the request was received.

Languages to be used for the exchanges of information

A request shall be submitted by a Member State's central authority in one of the official languages of the Member State being requested. The requested Member State shall reply either in one of its official languages or in any other language accepted by both Member States[18].

Content of notifications (data elements)

The ECRIS legal basis defines explicitly the minimum set of information that can or must be transmitted by the *convicting Member State's* central authority when notifying the Member State of the person's nationality of new convictions or of subsequent alterations and deletions of conviction information.

Obligatory information: the following information **must always** be transmitted, unless, in **individual cases** such information is not known to the central authority of the *convicting Member State*[19]:

i. Information of the convicted person: full name, date of birth, place of birth (town and State), gender, nationalities and, if applicable, previous name(s).
ii. Information on the nature of the conviction: date of conviction, name of the court, date on which the decision became final.

15 Council Framework Decision 2009/315/JHA – Article 8, paragraph 1

16 Council Framework Decision 2009/315/JHA – Article 8, paragraph 1(2)

17 Council Framework Decision 2009/315/JHA – Article 8, paragraph 2

18 Council Framework Decision 2009/315/JHA – Article 10

19 Council Framework Decision 2009/315/JHA – Article 11, paragraph 1(a)

iii. Information on the offence giving rise to the conviction: date of offence, name or legal classification of the offence, references to the applicable legal provisions.

iv. Information on the contents of the conviction: the sentence, any supplementary penalties, security measures and subsequent decisions modifying the enforcement of the sentence.

Optional information: The following information **shall** be transmitted **if available in the criminal records register**[20]:

i. Convicted person's parents' names;

ii. Reference number of the conviction;

iii. Place of the offence;

iv. Disqualifications arising from the conviction.

Additional information: The following information **shall** be transmitted **if available to the central authority**[21]:

i. Convicted person's identity number, or the type and number of the person's identification document;

ii. Fingerprints of the convicted person;

iii. Pseudonym and/or aliases.

Any other relevant information concerning the convictions entered in the criminal records may be transmitted if deemed necessary.

Content of replies (data elements) to requests for information

The ECRIS legal basis defines that from 27 April onwards, once ECRIS is operational, the Member States **must store** the **obligatory** and **optional** information listed above and received from other Member States for the purpose of including the said information on convictions into the replies to be provided to requests for information on convictions[22].

20 Council Framework Decision 2009/315/JHA – Article 11, paragraph 1(b)

21 Council Framework Decision 2009/315/JHA – Article 11, paragraph 1(c)

22 Council Framework Decision 2009/315/JHA – Article 7 (1)b & Article 5(1) and (2) & Article 11(1) and (2)

Format of information to be exchanged

The ECRIS legal basis defines standard forms for issuing requests and providing responses to such requests and to be used until the ECRIS application is operational[23]. These forms provide a standard grouped list of fields to be filled in.

From April 2012 onwards, the central authorities of the Member States shall transmit the information electronically using a standardised format[24]. This format is the subject of the ECRIS Council Decision 2009/316/JHA and should be agreed in detail by the Member States in the scope of the discussions on the ECRIS implementing measures within the Council.

The ECRIS legal basis defines a common codification for categories and sub-categories to be systematically used for classifying:

- § the name or legal classification of the offence and of the applicable legal provisions[25]
- § the penalties and measures[26]

The Member States shall always refer to the corresponding codes when referring to offences, penalties and measures in their transmissions. By way of exception, where an offence, penalty or measure does not correspond to any specific sub-category, the "open category" code of the relevant or closest category shall be used. In the absence of the latter, a generic category code shall be used[27].

In addition to the common classification described above, the legal basis defines also additional common parameters that may be used[28] for indicating:

- the level of participation of the person in the offence
- the level of completion in the offence
- the existence of partial or total exemption from criminal responsibility
- recidivism
- supplementary penalties

23 Council Framework Decision 2009/315/JHA – Article 6, paragraph 4 & Article 7, paragraph 5

24 Council Framework Decision 2009/315/JHA – Article 11, paragraph 3

25 Council Decision 2009/316/JHA – Annex A

26 Council Decision 2009/316/JHA – Annex B

27 Council Decision 2009/316/JHA – Article 4

28 Council Decision 2009/316/JHA – Article 4 + Annexes A & B

- security measures
- subsequent decisions modifying the enforcement of the sentence
- the nature and/or conditions of execution of the penalty or measure
- a non-criminal ruling

Logging and Monitoring

In order to coordinate the actions for the development and operation of ECRIS, the relevant departments of the Member States and the Commission shall inform and consult one another within the Council with a view to establish logging systems and procedures making it possible to monitor the functioning of ECRIS[29].

Statistics

In order to coordinate the actions for the development and operation of ECRIS, the relevant departments of the Member States and the Commission shall inform and consult one another within the Council with a view to establish non-personal statistics[19] relating to the exchange through ECRIS of information extracted from criminal records.

In order to ensure the **efficient** operation of ECRIS, the Commission shall provide general support and technical assistance, including the collection and drawing up of statistics[30]. The Commission shall also regularly publish a report concerning the exchange, through ECRIS, of information extracted from the criminal records based on these statistics[31].

Verification of Conformity

In order to coordinate the actions for the development and operation of ECRIS, the relevant departments of the Member States and the Commission shall inform and consult one another within the Council with a view to establish procedures verifying the conformity of the national software implementations with the ECRIS technical specifications[32].

29 Council Decision 2009/316/JHA – Article 6, paragraph 2(b)(i)

30 Council Decision 2009/316/JHA – Article 3, paragraph 7

31 Council Decision 2009/316/JHA – Article 7

32 Council Decision 2009/316/JHA – Article 6, paragraph 2(b)(iii)

Overall ECRIS Deadline

The Member States shall take the necessary measures to comply with the provisions of the ECRIS legal basis by April 2012[33].

This implies that the ECRIS system – in particular the interconnection software and the sTESTA network connections – must be operational in all Member States by then at the latest.

Additional Considerations

- The ECRIS legal basis defines clearly the data elements to be transmitted to the Member State of the person's nationality when notifying of new convictions or of subsequent alterations and deletions of conviction information. It is to be noted that, according to the legal basis[34], the data elements defined as "obligatory information" and "optional information" **must be stored** by the Member States' central authorities for the purpose of retransmission when replying to a request for information on criminal record data issued by another Member State.
- The ECRIS legal basis defines that once ECRIS is operational, replies to requests for information on criminal records must contain the convictions that were stored into the national criminal records registers as well as notifications on convictions and subsequent changes and deletions to conviction information **received after 27 April 2012**. This implies that if a notification is received after 27 April 2012 indicating a change to conviction information that has been notified to the Member State of the person's nationality **before 27 April 2012**, it must also be included in future responses to requests. However, if the information on the convictions provided as response to the request is not complete, the requesting Member State may not be able to properly understand and process the information.
- While the ECRIS legal basis defines specific data elements as being "obligatory", it does not necessarily imply that the corresponding technical fields, that will need to be defined in the *ECRIS Technical Specifications* messages to be sent between the Member States' ECRIS applications, will also be made mandatory. Indeed, the notion of "mandatory" applied to a technical interface between two software systems is very strict and **technically binding** between these two applications. In a case where a mandatory element cannot be filled in by an application, this system is then technically unable to send the message to another application since the technical interface prohibits it.

33 Deadline for Council Decision 2009/316/JHA: 07th of April 2012

Deadline for Council Framework Decision 2009/315/JHA: 27th of April 2012

34 Council Framework Decision 2009/315/JHA – Article 11, paragraph 2

NJR Project

General

NJR stands for "Network of Judicial Registers" and is a project launched at the initiative of several EU Member States which started in 2004 – thus several years before adoption of the ECRIS legal basis – with the common objective to interconnect their criminal/judicial registers electronically so as to speed up the exchange of information about convictions and thus improve prosecution.

The aim of the NJR project is thus not to establish a new organisation called "European Criminal Register"[35] nor to create another central database, but rather to electronically network national criminal/judicial records by harmonising formats and establishing standards for the exchange of information. This network aimed at providing the model for a pan-European network of national criminal/judicial registers.

The NJR project has managed to reach agreements on the judicial and technical aspects of the information on criminal records to be exchanged. Furthermore it has conceived a technical specification for these computerised exchanges and several Member States have successfully implemented the NJR interconnection software and are, since a few years already, successfully exchanging information on criminal records in a modern electronic way.

At the time of writing of this document, the latest NJR technical specification is in version v1.4.2. It has been implemented by Belgium, Bulgaria, the Czech Republic, France, Germany, Italy, Luxembourg, the Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain and the United Kingdom. Some of these Member States are not yet interconnected with all other project partners while some are still in a development or testing phase. In addition to these Member States, please note that the following Member States have not implemented the NJR technical specifications but are close observers of the NJR pilot project or of the *NJR Reference Implementation*: Greece, Estonia, Lithuania and Sweden.

[35] More specifically, it is not the aim of the NJR project to establish a new organisation of a European criminal register character.

A new version v1.5 of the NJR technical specifications is currently being elaborated, already taking into account some of the aspects of the ECRIS legal basis, so as to converge towards the future ECRIS system, as well as enhancements based on the return of experience of the project partners.
It must be noted at this point that the Commission's proposal, which became the ECRIS Council Decision referred to earlier, is directly inspired from the NJR project. In particular the decentralised principle, the IT architecture and the idea of using common codifications and categories for transferring key information have been taken over from NJR.

Approach

The approach of the NJR project is to foster collaboration among the Member State partners so as to reach common agreements on what information to be exchanged and on the technicalities for realising the computerised exchanges.
In practice, this is performed by 2 workgroups that manage, conceive and implement the NJR project:

- the "Technical Workgroup" defines the technical basis for the communication between the partners (underlying network structure, communication protocols, etc.) as well as the data structures (and their content) to be transmitted by the participating registers;
- the "Judicial Workgroup", responsible for considering the possibilities of (partial) translation of the message content transmitted between the participating registers and for dealing with other legal aspects of the data exchange and data processing

These workgroups are constituted of experts, technical and juridical, delegated from the partner Member States and meet on a regular basis. The members of both workgroups inform each other about their topics of interest or topics under discussion or development. Questions concerning legal as well as technical aspects are decided in common plenary sessions.
New partners are accepted into the NJR project if they comply with the base rules and guidelines that have been established in the NJR project.
It is to be noted in particular that new partners are usually being coached by one or more experienced NJR members so that the knowledge and experience can be reused. This coaching is done also on the IT-technical level while the new partner is implementing the NJR specification and testing its software application. In practice, this is done by a close and daily collaboration between the technical experts and, if necessary, even by an on-site visit of the more experienced experts to the experts of the new partner State. This coaching principle is well appreciated and recognised amongst the NJR partners as a successful way to help speed up the learning curve of new partner States.

It is also to be noted that an approach for testing and verification of conformity has also been established in NJR. Currently, a new software implementation in a country is first fully tested and validated against one already working and previously validated NJR software system (usually against the software system of the coaching State). Then lighter tests are performed with the other NJR partners, mainly for validating the technical set-up, configurations and connectivity.

Functional Principles and Concepts

Functional Architecture

The project partners of NJR have agreed to channel the electronic messages from one another's criminal record registers through each country's national register. The national register of each State acts as "head office" with respect to the communication between the judicial authorities of this State and the foreign register. There is thus one single authority in each State that operates the NJR system and that deals with the exchanges of information on criminal records with the other partnering States. In particular, any request for information to be sent from a judicial authority (public prosecutor's office, court etc.) to a foreign register taking part in the NJR project should follow the (electronic) channel from the requesting authority via its national register (acting as "head office") to the foreign register. The corresponding information from the foreign register is then to be returned using the same path – from the foreign register delivering the information via the national register of the requesting authority (as "head office") to the requesting authority itself.

The diagram below, courteously provided by the *NJR Functional Concept* document, illustrates how in NJR information (for example, a request and the corresponding register information) should be passed on within the framework of international mutual assistance after a request is submitted by a criminal prosecution authority:

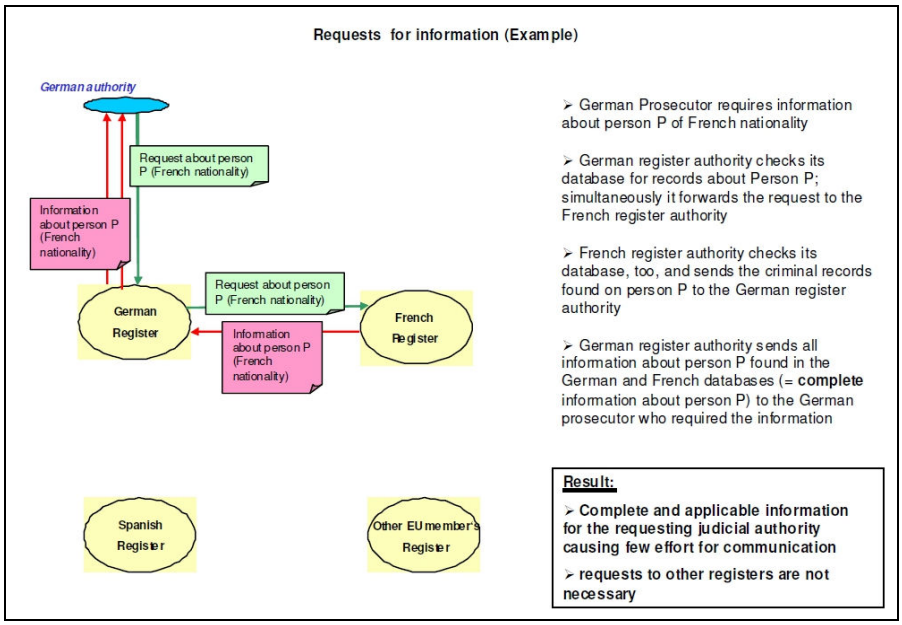

Figure 1 - NJR Request for Information

Functional Concepts for the Data Exchanges

First of all, the NJR system is to be viewed and understood as a **messaging system** that allows the transfer of information on criminal records between the central authorities of the partnering Member States.

Messages

NJR defines the following types of messages that can be exchanged:

1. Notification
   This message is sent by the *convicting Member State* to the Member State of the person's nationality in order to inform the latter of a new conviction or of a subsequent alteration or deletion of the conviction information.
   It foresees fields for carrying all necessary data related to the conviction: identification information of the person being convicted, information about the judicial decision, information on the offence, information on the sanction, supplementary penalties, security measures and subsequent decisions modifying the enforcement of the sentence, information on subsequent alterations and/or deletions of conviction information. The notification message is supposed to be processed and stored in the criminal record register of the receiving Member State.

2. Receipt
   The "Receipt" message is a Member State's response to a "Notification" message. In addition to indicating that the "Notification" message has been correctly processed, it is mainly used in NJR by the Member State of nationality for verifying that the "Notification" message was indeed sent by the *convicting Member State*. This allows checking in particular that no other entity has stolen the identity of a Member State for sending fake notifications.
3. Request
   This message is sent by the central authority of a Member State to the central authority of another Member State in order to request information and related data to be extracted from the criminal record of a person of the latter's register.
   Please note that, as described earlier, a judicial authority in a given Member State is not directly issuing such a request towards another Member State's central authority. It rather sends the request to its national central authority which transforms it into the commonly agreed NJR format and sends it on behalf of the judicial authority to the central authority of the requested Member State.
   The "Request" message foresees fields for carrying all data related to the request: information on the requesting authority, information on the purpose of the request, identification information of the person for which the criminal record is being requested
4. Information
   This message is the response that the requested Member State provides to the requesting Member State, following the processing of a "Request" message.
   It foresees fields for carrying all the data related to the possible answers that can be provided: information on the request that is being answered, identification information of the person for which the criminal record has been requested, information on the convictions (including information about the judicial decision, information on the offence, information on the sanction, supplementary penalties, security measures and subsequent decisions modifying the enforcement of the sentence, information on subsequent alterations and/or deletions of conviction information).

5. Error

   The "Error" message is a response to a "Notification", "Request" or "Information" message that a Member State can send back to the sender of the message either in the case that the processing of the message failed or for transmitting specific but exceptional functional responses resulting of the processing (such as "person died").

   It carries a set of fields that provide the cause of the failure partly in a common and codified manner and partly as free text elements.

Canonicalisation of the exchanged information

A major issue in such an information exchange system is to align the understanding of the information between the partners and guarantee a good level of quality for that information so that it can be processed effectively.

For this purpose, the NJR project defines and uses reference tables which provide classifications and codifications of values that are shared amongst the project partners. These allow for partial translation of the information: the "standardised element" needs only to be translated once, and then this translation can be stored in a database of the recipient and can be automatically added by the receiving register when transcoding the data records received into the format used by the end user.

It is also interesting to point out that these reference tables foresee, for each element, dates of validity (*valid from* and *valid until*) so as to take into account the fact that the values contained evolve in time.

Two types of reference tables are currently used in NJR:

- Common reference tables

  These reference tables are common to all NJR partners and their usage is compulsory. Their structure and content are defined in XML and are part of the NJR technical specifications. They are versioned together with the other technical artefacts of the NJR technical specifications.

  In the current version of the NJR specifications, common reference tables are used for:

  - identifiers of the transmitting registers
  - codes for countries and nationalities
  - categories of offences
  - currencies
  - error codes

Please note that in the version v1.5 of the NJR specification that is currently being elaborated, additional common reference tables are foreseen for the categories of penalties and measures as well as for various parameters.

§ National reference tables
These reference tables provide standardised codes that are specific to a given Member State. Their usage is optional but facilitates the understanding and processing of national information.

In the current version of the NJR specifications, national reference tables are used for:

- identifiers of the requesting authorities
- codes for the purposes of requests
- codes of offences
- codes for particulars of the decision
- codes for provinces

Languages, Translations and Transliterations

NJR is based on the principle that a Member State always sends messages in one of its official languages, character sets and alphabets. It is the responsibility of the receiving Member State to transform the data received in order to process it.

Please note that the definition in the NJR specification of structured data elements and especially common reference tables allow the NJR systems to automatically translate the data values into the language of the receiving Member States.

However, for free text elements such as freely typed remarks or additional unstructured information, no **systematic** automated transliteration or translation is performed nor is it part of the NJR technical specification. However, each Member State can freely develop such automations in its own national implementation of the NJR software system, as long as it complies with the commonly agreed NJR specifications.

IT Principles and Architecture

Architecture

The NJR partners have agreed to use the European sTESTA network as common communication infrastructure. The following diagram, courteously provided by the *NJR Functional Concept* document, illustrates the overall architecture of NJR (using only a few Member States as example):

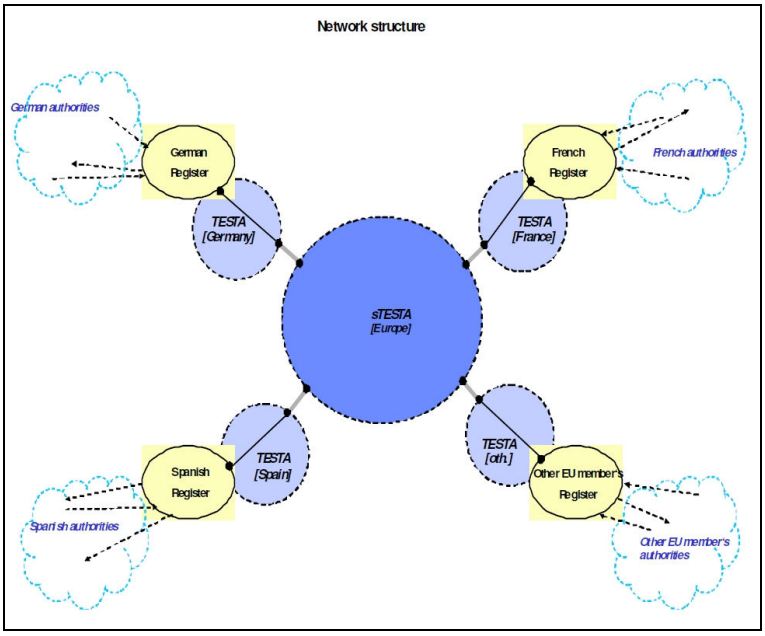

Figure 2 - NJR Network Structure

Technologies

The message exchanges between the NJR software systems are performed using *Web Services*.
The communication protocols are *HTTPS* (secure version of the HTTP protocol, used for the encryption of the messages, message negotiation and transmission over the network) and *SOAP* (***S**imple **O**bject **A**ccess **P**rotocol*, XML-based protocol specification for exchanging structured information in the implementation of *Web Services*).
The data packed into the messages is structured using *XML* 1.0 (***Ex**tensible **M**arkup **L**anguage*, a set of rules for encoding documents in machine-readable form). The definition of the messages and of their content is done in *XSD* (***XML S**chema **D**efinition*, one of several XML schema languages used to express a set of rules to which XML-encoded documents must conform to).

The *Web Services* are described using WSDL (***W**eb **S**ervices **D**escription **L**anguage* is an XML-based language that provides a model for describing *Web services*).
Unicode 4.0 (computing industry standard for the consistent representation and handling of text expressed in most of the world's writing systems) is used for the representation of all characters. More specifically the characters are encoded in the *UTF-8* (***8**-bit **U**nicode **T**ransformation **F**ormat*) format.
Please note that the XSD and WSDL definitions together determine the **IT-technical interface** that **must be respected** by the Member States' software systems in order to be able to actually exchange the information with each other. These interfaces are also commonly referred to as "service contract", since such interfaces are the **technically binding** elements between several software systems. Indeed, the electronic dialogue between two systems is rendered technically impossible if even a single rule described in these interfaces is not respected by one of the software systems.

Messaging Principles

In contrast to the **synchronous** technical communication, the communication on the level of the application, for example sending a request and receiving the corresponding information from the register addressed, is **asynchronous**. More specifically, a given *Web Service* call is performed in a synchronous way but the **functional** response to the call is provided asynchronously.
This approach makes it possible to deal with:

- Different internal rules used by the national registers for processing the information (such as for example, rules applied when searching for data records, manual work done by a person for identifying persons in cases of ambiguous search results etc.)
- Different durations for the treatment of the data by the national registers (such as for example using external translation services, performing further investigations for identifying a person, etc.)

The diagrams below, courteously provided by the *NJR Functional Concept* document, illustrate the principles of communication, considering technical and application level aspects, using the example of sending a request for information from the German to the Spanish register and receiving information (reply) upon this request:

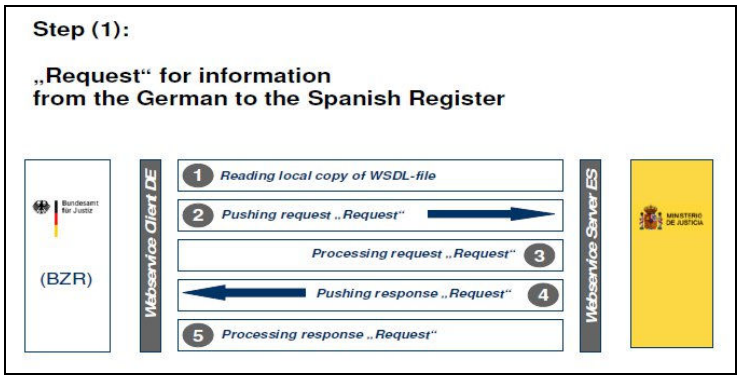

Figure 3 – NJR Messaging Example – Step 1 of 2

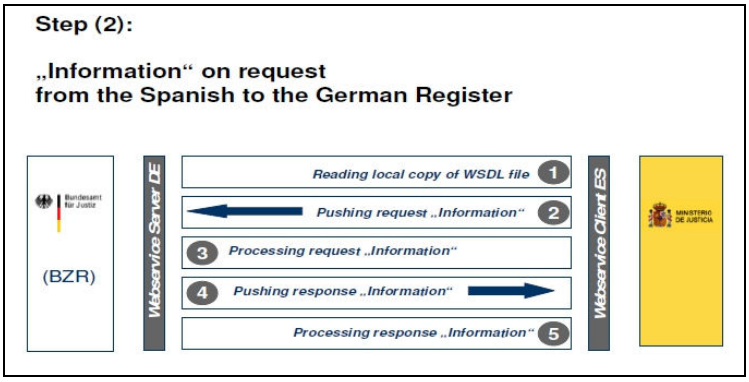

Figure 4 – NJR Messaging Example – Step 2 of 2

Comparison between ECRIS and NJR

The following sub-chapters elaborate on the similarities and differences that have been identified between the ECRIS legal basis and the NJR project. Please note that these are focusing on the aspects that are relevant for the establishment of the *ECRIS Technical Specifications*.

Similarities

As described earlier, the ECRIS legal basis is originally based on a proposal from the Commission which was directly inspired from the NJR project. As a result, the NJR system is in its nature and in many specific aspects very similar to the future ECRIS system and constitutes as such a solid and proven basis on which to build upon. Especially the functional architecture and concepts as well as the IT architecture and concepts can be reused as such. More specifically, the following similarities and/or equivalences have been identified:

- NJR has been designed as a decentralised information technology system. In particular, the criminal records data is stored solely in databases operated by the NJR partner States, there is no direct online access to criminal records databases between the NJR partner States and the interconnection software and databases storing, sending and receiving information extracted from criminal records are operated under the responsibility of the NJR State concerned.
- NJR is operated by the central authorities managing the national criminal records register in the partner States.
- NJR is using sTESTA as common communication infrastructure.
- Globally[36], the NJR "Notification" message corresponds to and fulfils the need described in the ECRIS legal basis for notifying the Member State(s) of the person's nationality of convictions and subsequent alterations and deletions of conviction information.
- Globally[34], the NJR "Request" message corresponds to and fulfils the need described in the ECRIS legal basis for issuing requests, for purposes of criminal proceedings, to other Member States for information and related data to be extracted from the criminal record of a person.
- Globally[34], the NJR "Information" message corresponds to and fulfils the need described in the ECRIS legal basis for providing responses to requests issued by other Member States for information and related data to be extracted from the criminal record of a person.
- NJR uses common and national reference tables for reducing the need of translation and for facilitating the understanding and processing of the data being exchanged. In particular, NJR features already a common reference table for categories of offences.
- The NJR specifications and software systems already define and carry the same data elements as the ones specified in the ECRIS legal basis, with the exception of fingerprints (see also section "Differences" below).
- In the NJR project, non-personal statistics are collected by all partner States. These statistics are then consolidated and regular reports are produced by a central body (currently this task is performed by the central authority of Germany).

Differences

Although the detailed ECRIS technical specifications still need to be elaborated, major functional differences have been identified between the future ECRIS system, as defined in the ECRIS legal basis, and the current NJR system. The following will thus need to be taken into account when designing the ECRIS technical specifications, in addition to the existing NJR specifications:

[36] "Globally" denotes the fact that, while a general equivalence between NJR and ECRIS has been identified, it does not imply that the NJR solution for this part can be reused exactly as such without applying changes. It is still necessary to further elaborate the details and, if necessary, adapt them in order to become ECRIS-compliant.

§ While NJR already defines a common reference table for the categories of offences, the content of this common reference table needs to be adapted in order to match annex A of the ECRIS legal basis[37].
(Please note that this table is currently being reviewed by the NJR members in view of elaborating version v1.5 of the NJR specifications and that this revision can be used as basis for drafting the ECRIS technical specifications.)

§ NJR, in its current version v1.4.2, does not yet define common reference tables for the penalties and measures. These need to be drafted and provided in XML.
(Please note that a draft proposal for such a table has been created by the NJR members in view of elaborating version v1.5 of the NJR specifications and can be used as basis for drafting the ECRIS technical specifications.)

§ NJR, in its current version v1.4.2, does not yet define common reference tables for the following parameters defined in the annexes of the ECRIS legal basis:
- the level of participation of the person in the offence
- the level of completion in the offence
- the existence of partial or total exemption from criminal responsibility
- recidivism
- supplementary penalties
- security measures
- subsequent decisions modifying the enforcement of the sentence
- the nature and/or conditions of execution of the penalty or measure
- a non-criminal ruling

(Please note that a draft proposal for such tables has been created by the NJR members in view of elaborating version v1.5 of the NJR specifications and can be used as basis for drafting the ECRIS technical specifications.)

§ The NJR structures, names and formats of the individual information elements that are contained in the messages to be exchanged do not necessarily comply with the standard forms described in the ECRIS legal basis. Although an exact and full compliance is not necessarily made mandatory (or even achievable) these data structures, names and formats would need to be revised.
Examples of such possible revisions could be:

[37] Council Decision 2009/316/JHA – Annex A

- renaming the field "Christian name" into "forename"
- revising the technical format and structure of date elements (for example, instead of using a text field constituted of 8 numeric characters, a structured XML element containing discrete fields for representing the year, month and day could be used)
- revising the structure of the field "purpose of the request" for purposes other than criminal proceedings

§ The ECRIS legal basis defines explicitly compulsory data elements, but also implicitly some data elements must be made compulsory so that the message exchanges can be operational and function as described in the ECRIS legal basis. Examples of such implicit compulsory data elements would be:

- the purpose of the request
- the indication whether a notification can be retransmitted as responses to requests for non-criminal proceedings

It is thus also necessary to revise the data elements that are made mandatory. This concerns approximately 25 specific data fields.

Please note however that, as explained earlier in section 2.2.2, the fields that are made mandatory from a technical point of view in the *Web Services* interfaces and XML definitions are **technically binding**. If such a field cannot be filled with a proper value in some cases, even exceptionally, then the message exchange cannot take place at all. This needs to be taken into account when deciding the data elements that need be made mandatory in the technical "service contracts" (i.e. technical interface, XML definitions, etc.). In particular, no all data elements defined as "obligatory" in the ECRIS legal basis can be made technically mandatory in the information exchanges.

§ The ECRIS legal basis defines explicitly the data elements that must be stored by the Member States for the purpose of retransmission upon request. In the NJR project, each Member State's central authority is currently freely deciding whether information is to be stored at all and if so, which data elements are to be kept and then later to be retransmitted, based on the capabilities of the criminal record register and national legislation. Thus in NJR, only information actually stored in the criminal records register would be retransmitted in response to a request, thus potentially leaving out convictions received earlier from other partner States but not stored in the register.

§ The ECRIS legal basis foresees the possible exchange of fingerprints[38], which is currently not supported in NJR.

§ The ECRIS legal basis foresees support for the "place of the offence", which is currently not supported in NJR in a structured form.

[38] Council Framework Decision 2009/315/JHA – Article 11, paragraph 1(c)(ii)

- The ECRIS legal basis foresees issuing requests for purposes other than criminal proceedings and especially defines the expected behaviour and responses to be provided to such requests. Currently NJR mainly deals with requests for criminal proceedings. As a result, compared to NJR, additional data elements and possible responses are to be defined for ECRIS, such as for example foreseeing a new message indicating that additional convictions are available but should be requested to other Member States.
- The ECRIS legal basis specifies explicitly that the deadlines for responding to requests are of 10 or 20 days, depending on the purpose for which the request was issued. In NJR, the deadline for responding to a request is set to 7 days while the deadline for responding to a notification is set to 21 days. Furthermore, in ECRIS the deadlines are expressed in working days and are to be counted from the date on which the request or additional information is received by the requested central authority. This implies that it is the receiving Member State's calendar which is to be considered (i.e. for public holidays, office closing days, etc.) and that the processing time is to be counted from the date of reception on the side of the requested Member State. In NJR, the deadline is expressed in calendar days and it is the date of sending that is used for starting the counter, thus on the side of the requesting Member State.
- The ECRIS legal basis defines explicitly that requests are to be sent in one of the official languages of the requested Member State. In NJR, all messages sent are issued in one of the languages of the sending State.

Please note that the ECRIS legal basis also imposes certain rules and behaviours to Member States' central authorities which were not necessarily applied in the NJR Project, such as for example **which** convictions must be retransmitted upon request for purposes of criminal proceedings or the fact that alterations and deletions notified by the convicting Member State must entail **identical** alterations and deletions in the information stored by the receiving Member State. These differences between ECRIS and NJR are however not being elaborated in this document since they do not affect the elaboration of the *ECRIS Technical Specifications*. Indeed, as explained later in this "Inception Report" document, it is the Member States' responsibility to ensure that the information being transmitted via ECRIS is correct, complete and that it complies with the provisions of the ECRIS legal basis. This cannot be enforced by the ECRIS software system.

Possible Enhancements

The return of experience from the NJR partners is also a very valuable input for elaborating the *ECRIS Technical Specifications* since it provides lessons learned gathered from real operational exchanges with the NJR software systems. While these are not differences between ECRIS and NJR, the design of the *ECRIS Technical Specifications* should also take into account the following items for enhancements:

- In NJR, the "Error" message and contained error codes are used both for functional and partly technical errors, leading in some cases to misunderstandings or more difficult processing. The separation between functional errors (such as identification not possible, person does not exist, response to request does not match with request, etc.) and technical errors (data elements missing, field has an unexpected value, etc.) can be revised. On a technical level, this is also made more complex due to the fact that the synchronous *Web Service* calls can also end up with a technical error such as for example a "SOAP Fault" or a "NACK" return message.
- In the functional "Error" messages, it has been reported that in some cases there is not sufficient information provided back in order to be able to actually correct the issue.
- In NJR, it is currently not possible to easily exchange several messages back and forth for the same request or notification, for example for establishing a dialogue involving several messages and responses for clarifying first the identity of the person before actually processing the request or notification.
- In NJR, it is difficult to clearly identify the ending of the dialogue between two NJR systems. For a "Request" message, the dialogue is supposedly closed either by the reception of an "Information" message, by a pre-defined time-out or by the reception of an "Error" message. However this error, depending on the error code, either closes the dialogue or asks the requestor to extend the pre-defined time-out. For a "Notification" message, the dialogue is supposedly closed either by the reception of a "Receipt" message, by a pre-defined time-out or by the reception of an "Error" message.
- In NJR, it is currently not possible for the sender to know, when a notification has been processed, under which identity information the conviction information has been stored in the criminal record register of the Member State of the person's nationality.
- NJR does not foresee the possibility to respond to a "Receipt" message. However in some cases it might still be necessary to reply for indicating errors such as for example that the "Receipt" message does not match any previous "Notification" message.
- The "Receipt" message is currently mainly used in NJR for authenticating the NJR system to which a message is being sent and is thus used as a replacement for client-side security certificates. This can also be revised in the security analysis that is to be elaborated in the scope of the *ECRIS Technical Specifications*.

- Several NJR partners reported difficulties in establishing connections with other partner States due to the numerous intermediate steps for setting up the sTESTA connections. In addition, each technical change triggers again delays for updating the configurations in all intermediate systems between the NJR server and the actual sTESTA national *Euro-Gate*. Furthermore, they also reported that in this set-up it is currently very difficult to trace problems when the connectivity with a specific Member State is disrupted.
- In the proposal that is being drafted by the NJR partners for the next version v1.5 of the NJR specifications, it is foreseen to revise the structure of the data elements for separating and clarifying information on the offence, on the penalty and information on subsequent decisions that modify the enforcement of the sentence. A mechanism for establishing relations between offences, sanctions and decisions is also foreseen since it has been identified that subsequent notifications informing of subsequent alterations or deletions would need to refer back to information previously transmitted. The design of the *ECRIS Technical Specifications* should also incorporate these ideas.

Approach

The following sub-chapters describe the approach that is proposed by the European Commission and iLICONN in order to elaborate the first version of the detailed *ECRIS Technical Specifications*.

Please note that the proposal for the approach is based on the Council's proposal for the ECRIS methodology, letter 11286/10, which was sent to the delegations of all Member States on 05th of July 2010.

General

The *ECRIS Technical Specifications* project has a very tight schedule. Indeed, several Member States requested for these detailed technical specifications to be ready by end of 2010 so as to have sufficient time for implementing the ECRIS software systems.

Due to this timing factor, but also due to the fact that several Member States have already made changes for setting up and implementing the NJR project, the general approach is to remain as close as possible to the NJR principles and specifications when designing the *ECRIS Technical Specifications*.

This project is also focusing solely on the IT-technical aspects of the ECRIS specifications, based on the Council decisions on ECRIS which provide the legal basis for the work. As such, the future ECRIS software should be viewed purely as a **computerised messaging system** for transporting information back and forth between the central authorities of the Member States.

In particular, it is not the aim of the *ECRIS Technical Specifications* project to elaborate legislative proposals, suggestions for agreements regarding judicial matters, suggestions for the harmonisation of procedures between the Member States or suggestions for the harmonisation of juridical and penal concepts between the Member States.

The *ECRIS Technical Specifications* project aims at producing the **first version** of the detailed technical specifications. Sufficient room for future evolution and flexibility must be engineered into the design of the *ECRIS Technical Specifications* right from the beginning, allowing the Member States experts to further adapt them later on and to produce new versions of these specifications. In particular, the design must feature generic mechanisms and take into account such possibilities as implementing future judicial agreements for adding new data elements, adding new reference tables, revising the rules to be applied to the data elements, etc. However, this first version of the detailed technical specifications will serve as basis for the implementation of the first version of the ECRIS software systems to be rolled out and operated by the Member States by April 2012.

Furthermore, ECRIS is defined as a decentralised system to be implemented and operated by the Member States central authorities. Therefore the approach chosen for elaborating the *ECRIS technical specifications* is that the Member States experts should commonly decide and agree on how to perform these exchanges. The general idea is thus that the European Commission and iLICONN act as facilitators and coordinators. Their objective is to collect information from the Member States experts and other relevant sources in view of producing reasoned proposals to be reviewed, commented and adopted (or rejected) by the Member States experts. The European Commission and iLICONN in no way intend to impose any solutions but will only provide proposals, opinions and expertise so as to help the Member States in choosing the most appropriate ways of exchanging the information on criminal records, within the boundaries set by the *ECRIS legal basis*.

Finally, the tight schedule mentioned earlier also has as a consequence that the various stakeholders need to adopt a pragmatic approach and flexible working methods as described in the next sub-chapter.

Stakeholders, Roles and Responsibilities

Persons and Entities Involved

The following stakeholders are involved in the *ECRIS Technical Specifications* project:

- The 27 EU Member States, represented by:
  - their delegations
  - the designated legal and technical experts (referred to as "Experts Group")
- The Working Party on Cooperation in Criminal Matters (referred to as "COPEN Working Party")
- The Council of the European Union and its Presidency
- The European Commission – DG Justice
- The iLICONN Consortium, in particular the Intrasoft International S.A. company
- Additional experts being knowledgeable about criminal records, about other European data exchange projects in the field of justice and mutual assistance in criminal matters or about specific IT matters related to ECRIS (such as for example sTESTA).

Roles and Responsibilities

According to the Council's proposal, letter 11286/10:

> In accordance with Article 6 of the Council decision 2009/316/JHA, COPEN Working Party is a relevant forum for consultation and it is to be complemented by meetings of the Commission's Experts Group on criminal records in which all the Member States are represented by their legal and technical experts (hereafter referred to as "the Expert Group").
>
> Discussions are to be carried out within the above two formats of experts gathering.

The iLICONN Consortium is the external contractor referred to in the Council's proposal and which has been awarded the execution of this project. The Consortium is expected to perform all necessary fact-finding tasks and to produce all deliverables of the *ECRIS Technical Specifications* project, in the boundaries defined by the *ECRIS Technical Specifications* contract that binds the iLICONN Consortium to the European Commission – DG Justice.

The "European Commission – DG Justice" is the contracting party for the *ECRIS Technical Specifications* project. It acts as coordinator and facilitator between the various stakeholders, supervises the work done by the iLICONN Consortium and ensures that the terms of the *ECRIS Technical Specifications* contract are being respected by the external service provider.

The Expert Group is expected to:

- Provide input to the European Commission and iLICONN staff
- If necessary, its experts will participate in conference calls and/or bi-lateral clarification meetings with the Commission and iLICONN staff
- Review the deliverables published by iLICONN on *CIRCA*
- Provide comments on the deliverables
- Discuss and agree on the implementation of the comments
- Participate in and revise the minutes of the Review meetings
- Review the updated deliverables on the basis of the implementation agreed in the Review meetings

The COPEN Working Party is formally responsible for the adoption of the final documents concluding each of the stages of preparatory works, as well as the adoption of the detailed *ECRIS Technical Specifications*. The evaluation and adoption of the final documents by the COPEN is to be performed in Council meetings, in accordance with the project calendar detailed later in this document.

The Council of the European Union and its Presidency are organising and hosting the COPEN Working Party meetings. They also act as coordinators and facilitators between the various stakeholders with a view to adopt the *ECRIS Technical Specifications*.

It is to be noted that all Member States are expected to appoint at least one delegate to participate in the Expert Group as well as be granted access to the *CIRCA* system. Accordingly, the experts are expected to subscribe to *CIRCA*, if not yet done. The experts nominated to participate in the "Expert Group" are also expected to participate in the meeting of the COPEN Working Party, in order to ensure the continuity of the work.

Project Phases

The *ECRIS Technical Specifications* project is subdivided in the phases that are described in the next sub-chapters. Each phase builds on the findings and outcomes of the previous phase.
Please note however that due to the time constraints, fast-tracking needs to be applied extensively in this project, meaning that the works of several phases are in practice performed partly in parallel and are overlapping.

Inception Phase

This phase is dedicated to the preliminary collection of general information and studies for understanding the context and establishing the common ground on which the technical specifications of the ECRIS system can be elaborated.
The main products of this phase are this document, the “Inception Report”, and the “Glossary” document.

Analysis Phase

This phase is dedicated to the more detailed analysis of specific ECRIS issues that have been identified during the "Inception Phase" in view of drilling down towards the detailed technical specifications. It focuses on:

- The overall technical architecture of the future ECRIS system: communication infrastructure, protocols, standards, technologies, technical guidelines, etc.
- The technical security aspects of the data exchanges: security requirements, usage of encryption, which standards, which security policies, security guidelines and procedures, etc.
- The functional aspects of the message exchanges: kinematics of the dialogues between the Member States, the possible alternatives and exceptions to be foreseen, the data elements to be transmitted, etc.

The main products of this phase are the "Technical Architecture" document, the "Security Analysis" document and the "Business Analysis" document.

Production Phase – Detailed Technical Specifications

This phase is dedicated to the following tasks:

- The analysis of the logging and monitoring of the future ECRIS system
- The analysis of the collection of non-personal data for establishing statistics
- The drafting of the detailed ECRIS technical specifications

The main products of this phase are the "Logging, Monitoring and Statistics Analysis" document, the "Detailed Technical Specifications" (these are constituted of a set of technical files and of explanatory documents) and a detailed "ECRIS-NJR Fit-gap Analysis" document.

Production Phase – Verification of Conformity

This phase is dedicated to the analysis and elaboration of procedures for verifying the conformity of the future ECRIS applications – both the *ECRIS Reference Implementation* and the national software implementations – with the detailed technical specifications.

The main product of this phase is the "Verification of Conformity Analysis" document.

This phase closes the *ECRIS Technical Specifications* project.

Working Method

Steps and Tools

As indicated earlier, due to time constraints, a pragmatic and direct working method is preferred in order to move forward efficiently through the project phases.

In particular, the working language used for the communication, the meetings and the drafting of all documents is English. The only exceptions are the COPEN meetings which are featuring interpretation services so that each participant can express himself/herself in his/her preferred language and the Expert Group Review meetings which **may** feature limited interpretation services, depending on the capabilities of the Institution organising them.

The products of the work performed by iLICONN – questionnaires, proposals, meeting minutes, final documents, etc. – are to be published on *CIRCA*. The following steps and tools are used for producing the project products:

1. In a first step, the iLICONN experts proceed to the collection of information from the Member States experts, from the European Commission experts and from other relevant sources using the following methods and tools:
   - On-site visits of the Member States' central authority handling the criminal records. Due to time constraints, it is however unfortunately not possible to visit all 27 Member States' administrations. As briefly indicated in the introduction of this document, and in view of preparing this document, the iLICONN staff has already performed 5 on-site visits to a group of selected Member States, the selection being based mainly on criteria of physical proximity and level of experience and implication in the NJR project. A provision for 5 additional visits is currently foreseen in the contract between the European Commission and iLICONN, to be scheduled in September and October 2010. The selection of the Member States' administrations to be visited will highly depend on the answers provided in the "Inception Phase Questionnaire" and on the comments provided on this "Inception Report" document during the review cycle.

§ Written procedures using detailed questionnaires and proposals.
The "Inception Phase Questionnaire" that has served for preparing this "Inception Report" is quite general and it is browsing through many topics related to ECRIS. The next questionnaires to be prepared will rather focus on specific topics that are identified and described later in this document.

Before drafting the formal products of the *ECRIS Technical Specifications*, iLICONN will also issue written proposals for some specific topics, based on preliminary input received from the various experts. Then these proposals will be circulated to the Member States experts, using *CIRCA* and e-mail notifications, and will allow collecting specific comments in view of choosing the most appropriate solutions.

§ Direct bi-lateral contacts with Member States experts.
When necessary, and in order to maximise the efficiency, the iLICONN experts will take direct contact with the Member States experts using means such as phone, e-mail or video-conference. This will typically be done for example for further clarifying specific answers or comments provided by a given Member State to a questionnaire or document. For each such direct contact, iLICONN will ensure that the European Commission is kept informed of the discussion and of its outcome.

§ Direct contacts with the European Commission experts, *NJR Reference Implementation* experts and other relevant sources of information.
Due to physical proximity, the iLICONN personnel has direct contacts with experts from the European Commission, with experts from the contractor currently developing the *NJR Reference Implementation* software but also with other experts who have been involved in various studies and similar projects in the field of justice and cooperation in criminal matters.

It is also to be noted that the experts who have previously worked on studies in the fields of criminal records - notably on the studies "Review of National Criminal Records Systems in the European Union, Bulgaria and Romania with the view to the Development of a Common Format for the Exchange of Information on Criminal Records" of 2006 and "Feasibility study: Establishment of a European Index of Convicted Third Country Nationals" of 2010 – are also involved as advisors and reviewers in the *ECRIS Technical Specifications* project.

§ It is also proposed to organise multi-lateral meetings with groups of a limited number of selected experts from Member States for discussing specific topics. This could for example be done for discussing the technicalities for exchanging fingerprints with the experts of the Member States which have the possibility and the intention of using this option.

It is to be noted that for each specific topic to be further analysed, iLICONN proposes a specific approach based on combinations of the tools listed above.

2. Once the information has been collected, the iLICONN experts proceed with the writing of drafts for the various products of the phases described earlier.
3. All proposals and drafts are then systematically submitted to all Member States experts for revision. For the main products of this project, the formal "Review Cycle" is then started.

Review Cycle

In view of the rather tight time lines, the working method for performing the examination and revision of the documents produced by iLICONN by the Member States is based on the combination of submission of written comments and Expert Group meetings.

The following "Review Cycle" is proposed:

Event	Schedule	Elapsed Time
The project artefact is published on *CIRCA* for review	T0	
All comments are available	T1 = T0 + 7 working days	7 working days
iLICONN's authors positions are published on *CIRCA*	T2 = T1 + 6 working days	13 working days
Expert Group Review Meeting	T3 = T2 + 3 working days	16 working days
Minutes of review meeting are published on *CIRCA* for review	T4 = T3 + 3 working days	19 working days
Comments on the minutes of Review Meeting	T5 = T4 + 2 working days	21 working days
Minutes of review meeting are published for acceptance	T6 = T5 + 2 working days	23 working days
Minutes of review meeting are accepted	T7 = T6 + 1 working days	24 working days
Updated project artefact is published on *CIRCA* on the basis of the comments implementation agreed at the Review Meeting	T8 = T3 + 10 working days	26 working days
The updated project artefact is approved by the Expert Group	T9 = T8 + 5 working days	31 working days
The project artefact is approved by the COPEN Working Party	T10 = T9 + MAX 20 working days	51 working days

Table 1 – Review Cycle

The European Commission reports back to the COPEN Working Party the findings, issues and conclusions of the Experts Group Review Meetings.

The meeting minutes are to be finalised by iLICONN, so that they can serve as a basis for an implementation agreement. They are dispatched after the meeting to the COPEN Working Party. Regarding the COPEN Working Party meetings in the Council, it is the intention to dedicate a large part of the meetings to the *ECRIS Technical Specifications* so that the appointed Member States experts can be present. Depending on the number of open discussion points that are raised during the *Review Cycle*, a full one-day session can be dedicated to ECRIS.

Project Calendar

General Project Calendar

As proposed by the Council in letter 11286/10, the project calendar is defined as follows:

Event	Agenda	Date
Delivery: Inception Report		30/08/2010
COPEN Meeting	Discussion and adoption of the Inception Report	27/09/2010
Delivery: Business Analysis Security Analysis Technical Architecture		27/09/2010
Expert Group Review Meeting	Business cases, security and architecture	19/10/2010
COPEN Meeting	Adoption of agreed documents	20/10/2010
Delivery: Detailed Technical Specifications ECRIS-NJR Fit-gap Analysis Logging, Monitoring and Statistics Analysis		05/11/2010

Expert Group Review Meeting	Logging, monitoring and statistics Detailed technical specifications	01/12/2010[39]
COPEN Meeting	Adoption of the Technical Specifications and procedure for the logging, monitoring and statistics	09/12/2010
Delivery: Verification of Conformity Analysis		07/12/2010
Expert Group Review Meeting	Conformity measures	11/01/2011[40]
COPEN Meeting	Adoption of the conformity measures	01/03/2011[40]

Table 2 – Project Calendar

It is to be noted that, due to timing constraints, no "Expert Group Review Meeting" is foreseen for the revision of the "Inception Report".

[39] This date has been postponed so as to give sufficient time to the Member States' experts for going through the author's position on the comments issued on the related deliverables.

[40] This date will need to be further confirmed under the upcoming Hungarian Presidency.

Detailed Calendar of the Review Cycles

Based on the previously defined project calendar and proposed Review Cycle, the following schedule is resulting:

Deliverables	Delivery T0	Experts Comments T0+7	Authors Position T0+13	Expert Group Review Meeting T0+16	COPEN Meeting	Updated deliverables T0+26	Experts Approval T0+31	COPEN Approval T0+51
Glossary Inception Report	30/08/2010	08/09/2010	16/09/2010	N/A	27/09/2010	05/10/2010	12/10/2010	09/11/2010
Business Analysis Security Analysis Technical Architecture	27/09/2010	06/10/2010	14/10/2010	19/10/2010	20/10/2010	02/11/2010	09/11/2010	07/12/2010
Detailed Technical Specifications ECRIS-NJR Fit-gap Analysis Logging, Monitoring and Statistics Analysis	05/11/2010	16/11/2010	23/11/2010	01/12/2010[41]	09/12/2010	13/12/2010	20/12/2010	17/01/2010
Verification of Conformity Analysis	07/12/2010	16/12/2010	07/01/2011	11/01/2011[42]	01/03/2011[42]	26/01/2011	02/02/2011	01/03/2011

Table 3 – Detailed Calendar of Review Cycle

[41] This date has been postponed so as to give sufficient time to the Member States' experts for going through the author's position on the comments issued on the related deliverables.

[42] This date will need to be further confirmed under the upcoming Hungarian Presidency.

Please note that the Member States experts' collaboration will be requested heavily during the months of September, October and November 2010. Indeed, while each month a Review Cycle is planned, at the same time the collection of information for the next phase's deliverables will need to be carried out. The experts will thus be asked to perform the revision of the deliverables but also at the same time to provide responses to questionnaires, to comment various proposals and to provide feedback for the preparation of the next products.

Please note also that for the "Verification of Conformity Analysis", the COPEN meeting and COPEN approval dates are set to the same day and mark the end of the *ECRIS Technical Specifications* project.

Alignment of NJR and ECRIS Projects

While the *ECRIS Technical Specifications* project is being carried out, the NJR project is also still on-going and improvements are foreseen to be implemented. Obviously, since the ECRIS systems will be operational at the latest only in April 2012, the Member States which are already interconnected through NJR will need to continue operating the NJR systems until shifting to the ECRIS system. As already indicated earlier, a new version v1.5 of the NJR specification is currently being drafted by the NJR members in order to converge towards the ECRIS legal basis. In particular, it is to be noted that the NJR Judicial Workgroup has foreseen to meet next on 14th of December 2010.

As described in the project calendar earlier, the timeline of the *ECRIS Technical Specifications* project is much shorter than the usual NJR timelines. Therefore, and since the topics being discussed are closely related, it is proposed that the NJR members fully focus on the finalisation of the ECRIS specifications first before resuming their work on the new version of the NJR specifications. It is proposed that the focus of the NJR experts is put on the technical but also on the judicial and functional levels. Then the NJR partners can pursue the elaboration of the NJR specifications v1.5, taking into account the technical and judicial agreements found for ECRIS, and implement the new versions of the NJR software systems if deemed necessary.

At latest after finalising NJR specification v1.5, and after the Judicial Workgroup meeting mentioned above, it is proposed that the two NJR workgroups be transformed into equivalent ECRIS workgroups, complemented with the experts of the Member States that were not yet part of the NJR project. From that point on, the ECRIS technical specifications will become the basis for the further discussions within the ECRIS workgroups. Please note that at the time of writing of this document, the roadmap for transforming the NJR workgroups into ECRIS workgroups is only a proposal which has not yet been decided and that needs to be discussed in the next NJR workgroup meetings.

In order for the NJR partners which are already operating a running NJR software system to have a smooth transition towards the ECRIS software system, the versioning principle that is being proposed in NJR v1.5 and which will also be a part of the ECRIS technical specifications needs to foresee that the NJR systems in versions v1.4.2 and v1.5 will need to evolve towards the ECRIS software system in version v2.0.

Project Scope

The following sub-chapters define the scope of the *ECRIS Technical Specifications* project. They further detail the expected content of the deliverables to be produced by iLICONN and which have been indicated as main outputs of the project phases described earlier.

When considering the scope, the reader must also keep in mind that the *ECRIS Technical Specifications* project is only one of the first steps towards the implementation of the ECRIS legal basis. Therefore, the tasks to be performed in addition to this project are also briefly outlined.

In Scope

The following sub-chapters describe what is included in the scope of the *ECRIS Technical Specifications* project.

These descriptions are only provided **as an indication**, so as to provide to the reader an overview of what is to be expected from this project and what products and tasks are not to be expected. This allows the stakeholders to focus on the job at hand for this project rather than deviating to subjects that should be dealt with at another moment in time.

In particular, the descriptions of what is expected to be in scope of the project do not have any contractual value. The *ECRIS Technical Specifications* contract binding the European Commission and the iLICONN Consortium remains applicable.

Project Deliverable – Business Analysis

The "Business Analysis" document[43] presents the ECRIS data exchanges between the Member States' central authorities from a non-technical point of view. It focuses on the functional aspects and judicial concepts of ECRIS and aims at determining the various steps of the processes to be fully or partly automated, how these automations are to be realised and the tasks that remain to be performed within the Member States' administrations.

In terms of workflow, this analysis determines the *kinematics* of the computerised dialogues between the Member States' central authorities by exploring the various business cases, alternative courses and business exceptions that can occur. It details all "what-if" scenarios in order to determine exactly all messages and possible cases that need to be supported by the detailed technical specifications. It also determines the policies and rules to be applied to the transmission of the messages, such as the possibilities to group messages, the functional time-outs, possible retries after failures or faulty processing of messages, actions to be performed after the maximum number of retries has been reached, etc.

The analysis also determines the "domain model", which defines exactly the set of information to be exchanged, and more specifically the types of messages and the data elements to be contained in each such message. It defines the common business and validation rules to be applied to each data element. It also identifies the data elements that can be standardised and be codified into reference tables.

In particular, it is foreseen in the scope of this analysis to define common categories for purposes of requests, elaborate and clearly define the parameter tables of annexes A and B of the ECRIS legal basis, define without ambiguity the personal data to be used for identification and define the response messages that can be expected in various business cases.

[43] Note for the NJR partners: this document is comparable in terms of purpose and content to the "NJR Functional Concept" document.

The objectives of the business analysis are:

- § to clearly define the key business concepts such as offence and sanctions parameters, categories of purposes of requests, person aliases, etc.; indeed the "Business Analysis" must ensure that these elements are understood in the same way by all stakeholders, not only on a technical level but also and **especially on the judicial level**
- § to ensure that the technical specification is in line with the functional needs and allows the organisational interoperability between the Member States' central authorities
- § to provide a common functional understanding of how to process the messages and their content
- § to minimise the need for additional transliteration and/or translation by standardising, structuring and codifying the data elements to be exchanged and avoiding as much as possible the usage of free text elements (please note however that it is not the aim of the *ECRIS Technical Specifications* project to define a solution for automating the transliteration and/or translation of the remaining free text elements)
- § to foresee sufficient messages and data elements in order to **facilitate** the identification of persons based on the nominal personal data that is being exchanged in notifications and requests

The business flows are described using EPC diagrams (***E**vent-Driven **P**rocess **C**hain*), the message exchanges are described using flowcharts and/or UML (***U**nified **M**odelling **L**anguage*) sequence diagrams and the domain model is described in UML class diagrams.

The formats proposed are self-descriptive and are very easy to understand, also for persons with no IT-technical background. In any case, all the diagrams are accompanied by exhaustive textual descriptions so as to avoid any misunderstandings or ambiguities.

Project Deliverable – Technical Architecture

This document describes the general technical architecture and major technical design choices upon which the detailed technical specifications are built. It provides:

- § a general view of the technical ECRIS system architecture
- § a brief description of the common network architecture to be used by the Member States' central authorities for exchanging the ECRIS data
- § the detailed list of technologies, standards, formats, tools, libraries and protocols to be used for the computerised ECRIS communications

- descriptions of the design choices and technical principles to be applied, such as for example:
  - the versioning principles and how to apply them
  - how to handle technical errors
  - how technical validation of the messages and of their content is expected to be handled
  - how transactional behaviour is to be applied
- performance and response time requirements to be supported

Please note that the bases for this work are the architecture and design choices that have been agreed upon in the NJR project (sTESTA network, usage of web services, encryption, XML messages and UTF-8 encoding of the texts). However this technical architecture might need to be adapted in order to support the specifics of ECRIS (for example for including support of fingerprints) and must also take into account the outcomes of the other analyses that are being carried out in the scope of this project (in particular the "Security" analysis and the "Logging, Monitoring and Statistics" analysis). Furthermore, the technical architecture must also take into account the integration with the IT infrastructures of the Member States' central authority and the possible usage of centralised technical artefacts (if any). The usage of such centralised technical artefacts is considered only for the elements that the Member States agree to share on a centralised level and is designed in such a way that avoids having a single point of failure for the data exchanges.

Open industry standards and mature, widely used, well-supported technologies, standards, formats and protocols are preferred choices.

Please note also that this project focuses only on the part of the ECRIS software system that is responsible for communicating with other ECRIS software systems. Obviously, the ECRIS software applications may also feature:

- one or more end-user interfaces to be manipulated by the personnel of the Member State's central authority
- internal technical interfaces towards the national criminal records register software systems
- an internal storage system such as a database
- internal workflows for guiding the end-users through the internal processing of the messages
- and other functions that are not directly dedicated to the exchange of information

Such elements that are internal to a national implementation of the ECRIS technical specification are clearly out of scope of this project and are not dealt with in the technical architecture.

Project Deliverable – Security Analysis

This document focuses on the technical security aspects of the data exchanges between the ECRIS software systems.

The term "security" refers in this context specifically to the confidentiality and the integrity of the information on criminal records that is being transferred between Member States' central authorities.

In particular, the objective of the "Security Analysis" is to define for ECRIS a technical architecture and security concepts that focus on protecting this information from unauthorised access, theft, corruption or any form of modification by unauthorised or untrustworthy individuals.

It must also be noted that, in IT security, 100% secure solutions do not exist and that a balance must be found between the efforts to be done for securing the systems and the risks to be accepted.

Therefore, establishing the requirements in terms of IT security is a major element since they define precisely the level of security to be achieved, with proper knowledge of the risks that are purposefully not being addressed and thus accepted. For the "Security Analysis" to be performed in the *ECRIS Technical Specifications* project, these requirements are broadly defined as follows:

§ The protection measures must focus on the **exchange of information** on criminal records **from the sender's ECRIS software system to the receiver's ECRIS software system only**.

In particular, it is thus assumed that the following aspects are to be addressed by the Member States:

– The internal national processing of the information sent and received (i.e. all the steps, systems and processes used before the actual sending of the information on one side and all the steps, systems and processes used after the reception of the information on the other side).

– The internal IT infrastructure of the Member State's criminal records registers (i.e. criminal records databases or mainframes, national and local networks, desktops of the central authorities' personnel, national and local servers, etc.).

§ The protection measures must focus on the **technical architecture** and **design principles** to be used for the **data exchanges** between **ECRIS software systems**.

In particular, it is thus assumed that the following aspects are to be addressed by the

Member States:

– The internal architecture and design principles to be applied to the implementation of other functionality of the ECRIS applications, such as for example the end-user interfaces made available to the personnel of the Member State's central authority, the internal technical interfaces towards the national criminal records register software systems, an internal storage system (e.g. database or internal file system), internal workflows for guiding the end-users through the internal processing of the messages and other functions that are not directly dedicated to the exchange of information, etc.

– The underlying hardware infrastructure such as networks, firewalls, routers, switches, hubs, servers, etc.

– The protective measures to be taken at the level of the **coding** of the ECRIS software. Indeed, software defects, bugs and logic flaws are frequent causes for software vulnerabilities. The secure coding practices are to be dealt with by the future implementers of the ECRIS software systems.

§ The protection measures must focus on the **confidentiality of the information**, ensuring thus that the receiver is indeed no other than the intended authority to which the messages have been addressed.

In particular, it is thus assumed that the following aspects are to be addressed by the

Member States:

– The measures for protecting the accesses to the criminal records register or ECRIS application from within a Member State's central authority. In particular, how the identification of the central authorities' personnel is to be handled by the ECRIS software is not covered by this "Security Analysis" but should be defined in the later security analyses for the implementation of the ECRIS applications.

– The measures for physically protecting and controlling the accesses to the offices and desktops from which the criminal records register and/or ECRIS application can be used from within a Member State's central authority.

§ The protection measures must focus on the **integrity of the information during the data exchange** from one ECRIS application to another one, ensuring thus that the data that has been received is indeed identical to the data being transmitted by the claimed sender.

In particular, it is thus assumed that the following aspects are to be addressed by the

Member States:

– The processing and transformations of data to be performed before actually sending it out through the ECRIS software on one side and after the reception by the ECRIS software on the other side.

More generally, it is **not** the aim of this "Security Analysis" to perform in-depth studies or audits of the security-related infrastructures, regulations, policies and practices of all 27 Member States.

In the light of the security requirements stated above, the "Security Analysis" document thus provides:

- A description of the roles and responsibilities of the different actors of ECRIS
- A high-level risk analysis.
  The scope of this risk analysis is to formally identify the threats that may affect the exchange of information on criminal records through ECRIS software. For each such threat, an evaluation of the impact and of the probability of occurrence must be estimated in order to assess the level of potential damage. This risk analysis includes the following steps:
  - Defining the assets to be taken into consideration
  - Determining the security needs in terms of confidentiality and integrity, using the ECRIS legal basis and business requirements
  - Identifying the relevant threats in the context of the ECRIS data exchanges
  - Identifying the vulnerabilities of the ECRIS software, from the perspective of the data exchanges from one application to another one only
  - Evaluating the risk exposure for each threat by (1) estimating the impact of each threat on the assets and their associated security needs, (2) estimating the probability that a threat may occur and (3) associating the impact and the probability for quantifying the risk exposure and thus determining the priority to be given to the prevention of the threat.
- Descriptions of the proposed security controls to be applied to the ECRIS data exchanges for avoiding or mitigating the security risks (such as for example the usage of specific protocols and standards, encryption, authentication mechanisms, etc.)
- Descriptions of the processes and procedures to be followed in order to ensure that the architecture and security concepts described earlier are applied correctly (such as for example the processes for issuing, transmitting and processing security certificates, conformity checks to be applied, etc.)

Please note that in NJR, the security principles are based on the following facts and elements which constitute the basis for the discussions to be carried out in the context of the ECRIS Security Analysis:

- The usage of the sTESTA network is already reducing the number of network-related threats since it is completely separated and isolated from the Internet and since all traffic from euro-gate to euro-gate is encrypted.
- NJR assumes that the national networks between the national sTESTA euro-gate and the national central authority are secured to a level that is sufficient for the needs of the exchanges of information on criminal records. It assumes that there is a sufficient level of mutual trust on each partner's infrastructures, procedures, processes and systems.
- In order to ensure an end-to-end protection of the transmitted information on criminal records, NJR foresees an additional level of encryption from NJR software system to NJR software system by using HTTPS.

Project Deliverable – Logging, Monitoring and Statistics Analysis

The "Logging, Monitoring and Statistics Analysis*"* is foreseen as a document containing the two distinct parts described below.

The objective is to produce proposals for (1) implementing logging systems and procedures in view of monitoring the functioning of ECRIS and for (2) establishing collection of non-personal data in view of producing statistics.

Logging and Monitoring

This part focuses on the logging and monitoring of the functioning of the ECRIS software system. The term "logging" refers in this context specifically to the tracing of events allowing to record information about the execution of the ECRIS data exchanges. The purpose of the logging and monitoring tasks is to detect and diagnose problems in the transmission of information on criminal records between ECRIS software systems so as to be able to take corrective actions.

Here again, the logging and monitoring analyses focus solely on the exchange of information from one ECRIS software system to another one, leaving out the implementation of other functionality of the ECRIS software systems such as for example the end-user interfaces to be manipulated by the personnel of the Member State's central authority, the internal technical interfaces towards the national criminal records register software systems, internal storage systems (e.g. database or internal file system), internal workflows for guiding the end-users through the internal processing of the messages and other functions that are not directly dedicated to the exchange of information, etc.

The analysis document includes:

- A description of the roles and responsibilities of the different actors of ECRIS in terms of logging and monitoring.
- A description of the messages and data elements to be specifically collected and monitored.
- Descriptions of the possible alternatives for the collection of this data and of the possible procedures for operating the monitoring of the ECRIS data exchanges.
- A description of the rules to be applied for considering whether a data exchange is operating correctly or not.
- A description of proposals for the possible automation of the logging and monitoring processes (including a list of which processes can be automated and how the automation could be realised).

Statistics

This part focuses more specifically on the collection of non-personal data for the purpose of establishing statistics. Gathering such statistics on the functioning of the ECRIS software systems and on the data exchanges on criminal records between the Member States' central authorities is actually one of the monitoring tools that allow to determine if the systems are effectively functioning properly and in accordance with the ECRIS legal basis.

Here also, the collection of statistics data is analysed only from the perspective of the exchanges of information on criminal records from one ECRIS software system to another one, more specifically on:

- Outgoing and incoming notifications of convictions or of subsequent alterations or deletions of information on convictions.
- Outgoing and incoming requests for information on criminal records.
- Outgoing and incoming responses to requests for information on criminal records.
- Outgoing and incoming error messages.

The collection of statistical data on other parts of ECRIS, such as for example the internal national processing of the criminal records information, is not considered in this analysis and can be done by each Member State individually if deemed necessary.

The analysis document includes:

- A description of the roles and responsibilities of the different actors of ECRIS in terms of the collection of non-personal data for establishing the statistics and access to such data.
- A detailed description of the messages and data elements to be specifically collected.
- Descriptions of the possible procedures and processes for the collection of this data from all Member States, for the consolidation of the statistics and for the drafting of regular statistical reports (including the definition of the periodicity of these tasks, of how and how long the statistical data should remain available, how and where data should be archived, etc.).
- A description of the rules to be applied on the messages and data elements for properly categorising and interpreting the information to be collected.
- A description of proposals for the possible automation of the statistics processes (including a list of which processes can be automated and how the automation could be realised).

Project Deliverable – Detailed Technical Specifications

The "Detailed Technical Specifications" is a set of technical files and explanatory documents that provide the physical blueprint for the implementation by the Member States' central authorities of the ECRIS software.

These technical files are defining the "service contract" which constitutes the technically binding elements that each ECRIS application must respect in order to be able to exchange messages and data. These define the technical interfaces, the input and output data structures and formats as well as basic rules and constraints. The technical files are physically materialising the results and agreements described in the "Business Analysis", the "Technical Architecture", the "Security Analysis" and the "Logging, Monitoring and Statistics Analysis" documents.

On the assumption that the ECRIS data exchanges are realised in *XML* and using *Web Services*, this "service contract" is typically constituted of the *WSDL*, *XSD* and *XML* files:

- The *WSDL* files actually define the *Web Services* in terms of operations, inputs, outputs, data elements and types, network endpoints and ports to be used.
- The *XSD* files define the messages and data elements to be exchanged in terms of constraints on the structure and content of XML documents, such as rules defining the order elements, data types and their cardinality, uniqueness and referential integrity.
- The *XML* files define the reference data values to be used, such as for example common and national reference tables.

The technical files are using the commonly agreed standards and formats and are independent from the programming languages, technologies, libraries and development tools to be used for the implementation of the ECRIS software.

The explanatory documents are a complement to the technical files and provide:

- Diagrams and detailed textual descriptions of the elements defined in the technical files, outlining the technical relations, constraints between groups of data, consistency and integrity rules to be implemented, technical errors, etc.
- Diagrams and detailed textual descriptions of the detailed technical sequences of messages and communication flows between the Member States' implementations of the ECRIS software systems.
- "Implementation Specifications": detailed textual descriptions of the minimum behaviour, logics and algorithms to be implemented in the ECRIS applications for being able to effectively exchange criminal records information that can be processed by the involved parties. These "Implementation Specifications" serve as a minimum set of technical requirements that the future ECRIS implementations – both the national software implementations and the *ECRIS Reference Implementation* – need to satisfy.

Project Deliverable – ECRIS-NJR Fit-gap Analysis

This document presents in more details the differences between the NJR technical specifications v1.4.2 and the ECRIS technical specifications, based on the outcomes of the previous works. In particular it outlines the parts of the NJR systems that can be reused as such or with minor adaptations. It provides, if possible, technical guidelines and proposals for migrating from the NJR software implementation to the ECRIS software implementation.

Project Deliverable – Verification of Conformity Analysis

This analysis aims at defining the procedures to be applied for verifying the conformity of the ECRIS software systems – both the national implementations and the *ECRIS Reference Implementation* – with the *ECRIS Technical Specifications.*

The analysis document provides the test management plan and includes in particular:

- A description of the roles and responsibilities of the different actors of ECRIS in terms of the verification of conformity.
- A detailed description of what exactly needs to be verified.
- High-level descriptions of the test scenarios, both functional and technical, to be conducted for verifying the conformity of the ECRIS software applications with the technical specifications (including scenarios for verifying the conformance with the security specifications as well as the conformance with the logging, monitoring and collection of data for statistical purposes)
- A description of the requirements for conducting the conformance tests, including requirements on staffing (number of persons and profiles), activities to be carried out before, during and after the tests, technical requirements (such as for example hardware, software, network connections, accesses, security certificates, etc.).
- A description of the possible procedures and processes for applying the conformity tests

- A description of the proposals, including possible alternatives, for the parts of the testing processes that can be automated by test robot applications.
- The acceptance criteria for the conformity tests.
- A description of the processes to be applied in case of non-conformity of an ECRIS software system.
- Types and formats of the conformance test reports.

Please note that the detailed test cases, which are the concrete physical implementation of the test scenarios including detailed input values and expected output values, are not part of this analysis.

Other Project Activities and Products

While the deliverables described earlier constitute the main products of the *ECRIS Technical Specifications* project, it is also interesting to briefly indicate that additional activities are to be carried out by iLICONN, as specified in the *ECRIS Technical Specifications* contract.

Such activities include for example:

- A limited number of additional on-site visits of the Member States' central authorities
- Contract management, project management and quality assurance activities in order to ensure to the European Commission and to the Member States that the terms of the *ECRIS Technical Specifications* contract are followed.
- Drafting and reviewing of minutes of meetings.

Out of Scope

The previous chapter described in detail the elements that are in the scope of the *ECRIS Technical Specifications* project. It is however interesting to explicitly identify and highlight some topics, issues and products that are not part of the scope so as to give the reader a better insight of the context.

Issues

The following list describes issues and aspects of the exchanges of information on criminal records that have been identified during the *Inception Phase* but that are out of scope of the *ECRIS Technical Specifications* project:

- During the preliminary study of the available input material and during the on-site visits, it appeared clearly that one of the major issues concerns the identification of the person based on the personal data that is contained either in a notification or in a request issued by another Member State. It is however not the aim of the *ECRIS Technical Specifications* project to define a common identification process to be applied internally by all Member States' central authorities. Indeed, the ECRIS system is only to be considered as a messaging system that should be used for transmitting as much relevant personal data as possible. The business analysis focuses on defining sufficient messages and data elements in order to **facilitate** the identification process, but it still remains the responsibility of the Member States to transmit complete and correct identification information and to apply the best possible techniques for uniquely identifying a person using the personal data that has been given.
- The *ECRIS Technical Specifications* project needs to propose a technical solution for the optional transmission of fingerprints between the central authorities of the Member States. However, there are several different formats and standards available for the electronic representation of fingerprints. There are also different approaches that can be applied for actually capturing the fingerprints and for evaluating matches. Such issues are out of scope of the project. Indeed, the solutions to be provided focus only on the transmission of the fingerprints data, including the definition of limitations in terms of file types and message sizes, but they do not aim at solving interoperability issues arising from different ways of understanding, interpreting and processing fingerprints data in the various Member States.
- While the *ECRIS Technical Specifications* project aims at reducing the need for translation of information, it is obvious that unstructured and non-standardised free text elements will still need to be transmitted between Member States. The automatic transliteration and translation of such data elements are out of scope of the project. It is indeed the Member States' central authorities' responsibility to transform the information in such a way that it can be processed correctly.
- During the "Inception Phase" it also appeared that the national sTESTA set-up and configuration is a major issue since it requires many interventions at different levels and on different networks in order establish operational connections between Member States' central authorities. Furthermore these multiple levels and networks also complicate the trouble-shooting activities when encountering connectivity issues. It is not the aim of the *ECRIS Technical Specifications* to solve these issues. However the architecture and design proposals to be elaborated will take these factors into account and will try to minimise the difficulties as much as possible (for example by proposing an architecture that is only very loosely tied to the network set-up so as to minimise the changes in the network configurations).

Additional Activities and Products

It is obvious that the *ECRIS Technical Specifications* project is just one of the steps that need to be performed in order to implement the ECRIS legal basis in all Member States. For the sake of clarity, this section briefly outlines some of the main activities and artefacts that will need to be carried out and produced in addition to the *ECRIS Technical Specifications*:

- Non-binding manual for practitioners
  As defined in the ECRIS legal basis[44], the non-binding manual for practitioners will address the procedures governing the exchange of information, in particular the modalities of identification of offenders, common understanding of the categories of offences and penalties and measures, and explanation of problematic national offences and penalties and measures, and ensuring the coordination necessary for the development and operation of ECRIS.

  In particular and especially since the *ECRIS Technical Specifications* can only define rules that are common to all Member States, this manual will need to describe the guidelines and practices to be followed in order to efficiently exchange information with other Member States, taking into account the specificities of each Member State. The following is a typical example of such guidelines which cannot be enforced in the *ECRIS Technical Specifications*:

  - Some Member States extensively use a national number for uniquely identifying persons. The *ECRIS Technical Specifications* cannot enforce the usage of such an identification number since many Member States do not have such information. However the manual for practitioners should clearly inform the end-users of the ECRIS system which identification number should be provided in notification and request messages for each such Member State in order to facilitate the identification processes.
- After the adoption of the first version of the *ECRIS Technical Specifications*, one or more centralised management and coordination structures will need to be established in order to perform recurrent tasks such as:
  - The storage, publication and maintenance of the technical specifications and related documentation.
  - The organisation of technical and judicial ECRIS workgroups for the elaboration of the future versions of the technical specifications and software systems, for discussing matters related to the content of the information exchanges and for evaluating the effectiveness of the ECRIS software from the end-users point of view.

[44] Council Decision 2009/316/JHA – Article 5, paragraph 1

- Various coordination and communication activities such as following up on the progress with appointed Member States experts, acting as single point of contact for matters related to ECRIS, acting as point of contact for sTESTA issues and consolidating the collected non-personal data for drafting the statistics reports.
- Hosting, implementing and maintaining technical artefacts used by the ECRIS software systems (if any).
- Hosting, implementing and maintaining common IT tools for ECRIS (such as for example setting up a centralised bug tracking/issue tracking tool like JIRA for registering the requested changes and fixes to be brought to the ECRIS technical specifications).
- Consolidation of non-personal statistical data and associated reporting.

For each such centralised entity, it will be necessary to clearly define its role, responsibilities and working procedures.

§ After the adoption of the *ECRIS Technical Specifications*, a set of organisational and technical guidelines on how to set-up and troubleshoot sTESTA connections and an sTESTA DNS should be drafted.

§ In order to comply with the ECRIS legal basis, several Member States need to apply legal and structural changes, in particular changes of their national legislation, changes of the working procedures and of the organisation of the authorities that are handling criminal records, changes to the internal IT infrastructures such as the criminal records register itself, etc.

§ The detailed test cases for the verification of conformity of the ECRIS software systems will need to be elaborated.

§ The European Commission will need to procure the works for the production of the *ECRIS Reference Implementation*.

§ The Member States will need to implement the ECRIS software systems, either by upgrading their existing NJR application, by developing a brand-new ECRIS application from scratch or by installing and customising the *ECRIS Reference Implementation*.

Assumptions and Constraints

The following chapter provides the assumptions and constraints that have been identified during the preliminary studies of the ECRIS legal basis, *NJR Pilot Project*, on-site visits of a series of Member States' central authorities and responses to the "Inception Phase Questionnaire".

These assumptions and constraints provide the ground on which the further works for the *ECRIS Technical Specifications* project are being elaborated. The future analyses, discussions, proposals for solutions and other products of this project use these as basis and assume that these hypotheses and constraints remain valid at all times.

Please note that some of these assumptions and constraints are not necessarily true at the moment of writing of this document. However they will need to be true for operating the ECRIS systems successfully as from April 2012 onwards.

General

[AG-1] It is assumed that, even if Member States appoint several central authorities for handling the exchanges of information on criminal records, that there is only **one single entity operating the ECRIS software**. In particular, it is assumed that this single entity is the only one acting as single point of contact for all communications between the central authorities of this State – both judicial and non-judicial – with the criminal records registers of other Member States using ECRIS.

This implies that a Member State's central authority can thus address its notifications, requests and responses to requests to a single entity and to a single ECRIS software application of another Member State's central authority, which is then redirecting the messages internally to other national authorities if necessary.

[AG-2] It is assumed that ECRIS is a decentralised system, in the sense that the storage of the criminal records information is not centralised but managed individually in each Member State.

[AG-3] It is assumed that each Member State's central authority stores the criminal records information, especially also the notification of new convictions, subsequent alterations and deletions of conviction information coming from other Member States, in accordance with the provisions defined in the ECRIS legal basis.

[AG-4] It is assumed that each Member State's central authority extracts from its criminal records register all conviction information and sends it to other Member States in response to requests as specified in the ECRIS legal basis.

[AG-5] It is assumed that the information on criminal records transmitted by each Member State's central authority to foreign Member States' central authorities is always **correct and complete**. In particular, it is assumed that the necessary legal and functional verifications as well as the quality control of the conviction information have been done by the Member State's central authority before sending out the information towards other authorities.

Please note that the "completeness and correctness of information" described in this assumption is considered from a functional point of view rather than from a technical standpoint. Indeed, it **is** in the scope of the *ECRIS Technical Specifications* to ensure a certain degree of **technical correctness and completeness** of the data to be exchanged between Member States' central authorities, such as for example that all mandatory fields are filled in properly, that fields contain values that respect the formats and structures defined in the technical specifications, etc. However it is the Member States' responsibility to ensure for example that the names of persons provided are correct (i.e. correct spelling) and complete (i.e. all available last names are provided), that all applicable convictions stored in the criminal records register are indeed being transmitted in accordance with the legislation (i.e. that the applicable retention and weeding rules are applied correctly, that no convictions information is forgotten or omitted by mistake), etc.

[AG-6] It is assumed that the ECRIS software applications – both the national software systems and the *ECRIS Reference Implementation* – fully comply with the *ECRIS Technical Specifications*.

[AG-7] It is assumed that the personal data being transmitted between the Member States' central authorities is used by these authorities in accordance with the ECRIS legal basis and with the provisions of the applicable data protection regulations.

[AG-8] It is assumed that the only messages exchanged via the ECRIS software systems are the ones defined in the *ECRIS Technical Specifications*. In particular, it is assumed that the Member States will not implement additional custom messages in order to fulfil specific bilateral or multi-lateral agreements that have not been previously agreed by all Member States.

Functional

[AF-1] It is assumed that the ECRIS data exchanges are always performed as a dialogue between exactly two Member States' central authorities.
This remains also true in the specific case where a request is issued by Member State "A" towards Member State "B" for purposes other than criminal proceedings and that Member State "B" has convictions from another Member State "C" that cannot be disclosed. In this specific case, it is assumed that Member State "B" replies to Member State "A", indicating to "A" that additional convictions can be requested from Member State "C", and that the dialogue ends at that point. Member State "A" can then issue a new request towards Member State "C", **as a new dialogue**, in view of receiving these other convictions[45].

[AF-2] While the technical message exchange calls may be performed synchronously, it is assumed that the **functional** response to a message is always provided **asynchronously**. In particular, the following responses are to be provided in an asynchronous manner:

- A response to a notification of a new conviction or of subsequent alterations or deletions of information on convictions.
- A response to a request for information on criminal records.
- A **functional** error message as a response to any other message.

[AF-3] In the ECRIS data exchanges, it must be possible to uniquely identify across all Member States:

- A "notification" message
- A "request" message
- A "response to request" message
- A block of information on the identity of a specific person
- A block of information on a specific conviction
- A block of information on a specific offence
- A block of information on a specific sanction
- A block of information on a specific *judicial decision* (e.g. a decision of a new conviction, a decision bringing a change to a previous conviction, a decision affecting the execution of a penalty or measure, a decision grouping several previously determined sanctions into an overall sanction, etc.)

[45] Council Framework Decision 2009/315/JHA – Article 7, paragraph 2, 3rd subparagraph

[AF-4] In the ECRIS data exchanges, a "response to request" message must carry specific information so that a unique link to the "request" to which it provides an answer can be established (such as for example a unique number identifying the "request" message).

[AF-5] It is assumed that the official calendar of the **requested Member State** is taken into account for calculating the deadline for responding to a request for information on criminal records.

[AF-6] It is assumed that in each notification of a change or deletion concerning information on convictions previously sent to a foreign central authority, the sending Member State retransmits all historical information[46] stored about this conviction, and that is available in its criminal records register, rather than only sending the latest change or deletion.

[AF-7] It is assumed that the following data elements concerning a request for information on criminal records can **always and under all circumstances** be provided by all Member States' central authorities:

- the name of the requesting authority
- the purpose of the request

[AF-8] It is assumed that the following set of identification information of the person concerned by an ECRIS message can **always and under all circumstances** be provided by all Member States' central authorities:

- at least one first name
- at least one last name
- the year of birth
- at least one of the person's nationalities (please note that extremely rare cases have been reported where the person's nationalities is not stored in the criminal records register; these cases are however so exceptional that is has been agreed to leave this assumption)

[AF-9] It is assumed that the following set of information related to a *judicial decision* can **always and under all circumstances** be provided by all Member States' central authorities:

- date of the *judicial decision*
- name of the judicial authority that took the decision

[AF-10] It is assumed that the following set of information related to an offence can **always and under all circumstances** be provided by all Member States' central authorities:

- name of the offence
- category of the offence, in accordance with the annexes of the ECRIS legal basis
- date of the offence

[46] Note for the NJR partners: this refers to the « snapshot » approach which is also the approach that is applied in NJR.

[AF-11] It is assumed that the following set of information related to a sanction can **always and under all circumstances** be provided by all Member States' central authorities:

- name of the sanction
- category of the sanction, in accordance with the annexes of the ECRIS legal basis

Technical

[AT-1] It is assumed that all computerised ECRIS data exchanges are performed only on the sTESTA network.

[AT-2] It is assumed that no direct electronic interconnection is established between the criminal records register of the Member States.

[AT-3] It is assumed that each Member State's central authorities operate **one and only one single instance** of the ECRIS software application for exchanging the **real** information on criminal records with other Member States' central authorities (i.e. "real" information being the data really stored in the Member States' criminal records registers as opposed to dummy test data). It is further assumed that, in addition to the single production instance, several other instances of the ECRIS software can be operated for development and testing purposes.
(Please note that the wording "single instance of the ECRIS software" is meant here in the logical sense. In particular, this assumption does not exclude physical duplication of the hardware devices running the ECRIS software for implementing high-availability clusters or load balancing.)

[AT-4] It is assumed that the ECRIS software systems are performing the message and data exchanges using the following standards, technologies and protocols:

– *Web Services*

– *XML*

– *Unicode* and more specifically *UTF-8*

Please note that during the "Inception Phase", other alternatives such as messaging queues, workflow systems, secured e-mails and other standards and protocols have been evaluated.

However, the proposed technologies listed above appear most reasonable in order to remain close to the NJR architecture as well as flexible and easy to implement in many different programming languages and development platforms.

Please note also that the versions or implementations of the standards defined above, as well as complementary standards, protocols, formats and technologies are to be defined later in the "Technical Architecture".

[AT-5] It is assumed that the transactional feature of rollback of a message sent to another Member State is not required and does not need to be supported in the ECRIS data exchanges.

[AT-6] It is assumed that each Member State must be able to freely choose the tools, techniques, technologies and programming languages for implementing the *ECRIS Technical Specifications*. Therefore, it is assumed that the *ECRIS Technical Specifications* must be based on mature, well-supported and widely used industry-level technologies, standards, formats, and protocols that are as much as possible independent from specific development platforms, specific programming languages and vendor-specific solutions.

Security of ECRIS Data Exchanges

[AS-1] It is assumed that all Member States trust each other to apply the necessary protection measures in their national networks, infrastructures, policies and regulations in order to ensure a level of IT-security that is deemed adequate by all involved parties. In particular, it is assumed that:

– All Member States trust each other on the fact that they apply protection measures on all the networks between the server running the ECRIS software system and their national sTESTA euro-gate server to a level of security that is deemed adequate by all.

– It is assumed that all Member States protect the physical access to their IT infrastructure, and in particular the access to the criminal records register and to the ECRIS application, to a level of security that is deemed adequate by all.

[AS-2] It is assumed that the usage of the sTESTA network complemented by (1) end-to-end encryption of the messages sent by the ECRIS software systems and by (2) mutual authentication of the sending and receiving ECRIS applications is deemed sufficient by all Member States for protecting the confidentiality and integrity of the criminal records information that is being exchanged electronically between the Member States' central authorities.
(Please note that this assumption does not imply specific IT-technical implementations. In particular, it does not necessarily imply that the usage of HTTPS and mutual authentication using client- and server-side security certificates is made mandatory. Alternative technical implementations reaching the same objectives may be defined in the *ECRIS Technical Specifications*.)

[AS-3] It is assumed that the IT-security rules and policies that are applied to the ECRIS software systems for the exchange of information between Member States' central authorities apply to **all instances** of the ECRIS applications.
In particular, regarding instances of ECRIS applications that are operated for development and test purposes only, the same IT-security rules and policies as for the production instances apply **when referring to the protection of the availability** of the IT systems, especially when these tests imply communication with other Member States so as to not endanger the IT infrastructure of these other Member States. However, in terms of the protection of the confidentiality and of the integrity of the data, the development and test instances do not require the same level of security since these use dummy data.

[AS-4] It is assumed that the usage of cryptography and encryption algorithms in the context of the ECRIS data exchanges is considered as legal by all Member States.

Topics Requiring Further Analysis

The following chapters describe specific themes that have been identified during the "Inception Phase" and that require special attention and maybe even a specific approach in view of finding the most appropriate solutions in the *ECRIS Technical Specifications*.

For each theme, the sub-chapters describe briefly why it has been identified as requiring special attention and propose a specific approach.

Themes

Technical Architecture

The "Technical Architecture" of the ECRIS data exchanges is already identified as a specific deliverable of this project. However it has also been identified as a theme requiring special attention since it requires a specific approach in order to identify the most appropriate solutions to the following issues:

Versioning

Firstly, the term "version" refers in this context specifically to the version of the technical specifications and not to the version of the software implementation of these specifications.

One of the major issues identified already in NJR and that also needs to be taken into account in ECRIS is that the technical specifications will necessarily evolve in time and thus need to be conceived in such a way that the Member States can deploy their software implementations independently from each other, avoiding that for each change all 27 Member States would need to deploy the implementations at the same time and in perfect synchronisation.

The idea is thus that the ECRIS software implementations must support at any given time at least two versions of the technical specifications so as to provide sufficient flexibility for developments and deployments. One of the difficulties is however that the data structures and rules defined in the XSD files may change in subsequent versions of the specifications.

In particular, for the XML messages containing notifications that have been received under previous versions of the specifications and which have been stored locally for the purpose of being retransmitted upon request, the ECRIS applications will still need to be able to process and retransmit the information contained in these XML messages in a way that is technically compliant with the supported version of the specifications at this moment in time.

Let's take a concrete example:

The ECRIS software system of a Member State has received and stored subsequently for the same person:

- An XML message of a foreign conviction, using version v1.0 of the specification;
- Later on another XML message for notifying an update of the conviction information, using version v1.2 of the specifications;
- Still later on, another XML notification informing of a new conviction on the same person, using version v1.4 of the specifications.

Let's now also assume that, due to the national legislation of the Member State, the information contained in these notifications could not be registered in the criminal records register. If the Member State needs to respond later on to a request for information on the criminal records of that same person in the context of criminal proceedings, using the ECRIS specifications v1.5, the ECRIS software will need to send as response the following information:

- An XML message in v1.5 containing all conviction information stored in the criminal records register;
- The content of the XML messages stored for the purpose of retransmission in versions v1.2 and v1.4 (according to the assumption [AF-6] made earlier, the message in version v1.2 contains also the information provided in the message in v1.0 since all historical data is being transmitted along with changes).

sTESTA Connectivity

During the "Inception Phase", the setting up of the sTESTA connections, their monitoring, the application of configuration changes and the trouble-shooting of connectivity problems have been raised as being a major difficulty.

The proposed approach is to focus specifically on these issues in the context of the "Technical Architecture" and to proceed as follows:

- iLICONN prepares a description of technical proposals for the technical architecture, specifically targeting these issues
- The European Commission transmits these proposals to all Member States' IT experts for revision, using CIRCA.
- Based on the feedback received, the European Commission organises **a workshop** in Brussels **with a limited and reduced number of IT experts** from the Member States in order to reach a preliminary agreement on the proposals to be retained for the "Technical Architecture" analysis.

Security of the ECRIS Data Exchanges

As indicated previously, the ECRIS security measure focus on the usage of end-to-end encryption of the messages and data to be exchanged using the ECRIS applications and on the authentication of the sender and receiver.

NJR is based on the HTTPS protocol. The security certificates are used for establishing encrypted communication channels but the authentication is done **unilaterally** using the server-side security certificates only. **Mutual authentication** is currently not supported for a **single** message exchange, which implies that the origin of an incoming message is not verified. This is, to a certain extent, counterbalanced by using the NJR "Receipt" message as follows:

- § NJR system "A" sends a notification to NJR system "B".
- § "A" actually identifies "B" by its server certificate when establishing the SOAP transaction for sending the notification through the usage of the TLS protocol.
- § However the sender could have usurped the identity of sender "A". In order for "B" to verify that the sender is actually really "A", "B" sends a "receipt" message to "A". This time, "B" identifies "A" by its server certificate when establishing the SOAP transaction for sending the receipt through the usage of the TLS protocol.
- § This implies that if "A" receives unexpectedly a "receipt" message, the sender was not "A" but has stolen "A"'s identity.

This scenario shows weaknesses, such as for example:

- § "B" is made aware that "A" received the "receipt" message by the positive SOAP response. However "B" may not be made aware that "A" actually received it **unexpectedly**. "B" may thus not come to know that the identity of "A" has been stolen. NJR indeed relies on the fact that "A" has implemented a proper monitoring for verifying that the receipts actually really match notifications previously sent. NJR assumes that "A" is capable to detect such problems and raise a flag so that "B" can be manually informed that there is a problem and that investigations on a potential security breach can be performed. This may however not be the case.
- § "B" has already read the incoming "notification" message before sending the "receipt" message for verifying the identity of "A" (i.e. the synchronous SOAP call of the notification must be completed and return before "B" can send the SOAP call for the "receipt"). This creates vulnerability to various types of security attacks such as for example *denial-of-service* attacks. In particular, it is possible in this design to bombard the NJR system of "B" with fake "notifications" and render "B"'s system incapable of executing any other calls.

NJR also does not define a policy for the issuing, storage, publication and validation of these TLS certificates. As a result, some implementations of NJR do not validate the server certificates that they receive. Furthermore no third party, mutually trusted, certification authority is used in NJR. In

addition, the security certificates contain also the server's IP address and hostname, which implies that they are tied to the sTESTA network configuration. If this configuration needs to be modified, the security certificates need to be reissued, redistributed and reinstalled.

In view of the aspects mentioned above, it is proposed to revise the usage of HTTPS and evaluate possible variations of the NJR set-up, such as for example using mutual authentication with client- and server-side certificates, replacing the usage of HTTPS altogether in favour of other types of application-level encryption methods, etc.

The proposed approach is to focus specifically on these aspects in the context of the "Security Analysis" and to proceed as follows:

- § iLICONN prepares a description of technical alternatives for securing the data exchanges, specifically targeting the issues mentioned above.
- § The European Commission transmits sends them to all Member States' IT experts for revision, using CIRCA.
- § Based on the feedback received, the European Commission organises **a workshop** in Brussels **with a limited number of IT experts** from the Member States in order to reach a preliminary agreement on the proposals to be retained for the "Security Analysis". (Please note that in order to minimise the travels of the Member States' IT experts, this workshop could be combined with the workshop on the "Technical Architecture".)

Electronic Exchange of Fingerprints

As described earlier, the exchange of fingerprints is an option that is not supported in the NJR project and that needs to be addressed in ECRIS.

This specific subject requires further discussions and studies in order to clarify exactly what needs to be transmitted between the Member States that wish to use this option. This can range from sending only references to fingerprints that are stored elsewhere (thus implying that the Member States retrieve them with ad-hoc processes outside of the ECRIS data exchanges) to the physical attachment of the electronic fingerprint files to the ECRIS messages. In this second case, technical limitations need to be evaluated and defined, especially in the fields of file sizes and file formats.

The proposed approach is the following:

- § iLICONN collects additional information on the possibilities for exchanging fingerprints through direct contacts with selected Member States experts (i.e. the experts of the Member States which have indicated their intention to use this feature). Based on this input, iLICONN drafts specific alternatives for realising the exchange of fingerprints.
- § The European Commission transmits these alternatives to the concerned Member States for revision, using CIRCA.

- Based on the feedback received, a specific proposal is drafted and included in the "Technical Architecture" or "Detailed Technical Specifications" for revision and adoption by all Member States.
- If necessary, the European Commission **may** organise **a workshop** in Brussels **with a limited and reduced number of experts** from the concerned Member States in order to reach a preliminary agreement.

Business Analysis

The "Business Analysis" is considered as a critical task and is therefore identified as a specific deliverable of this project. It has also been identified as a theme requiring special attention since it requires a specific approach.

Please note indeed that in the NJR pilot project, the judicial and technical workgroups are meeting separately. For the *ECRIS Technical Specifications* project, the proposed way of working is that during the "Review Cycle" of the "Business Analysis", in each Member State, both **technical and judicial experts** perform the revision of the "Business Analysis" document and issue comments. Then, the comments received from the Member States are analysed by the author of the "Business Analysis" and the point of view of the author is provided to the Member States. At this stage, the comments should have revealed parts of the analysis on which there are judicial disagreements or which are still unclear from a business point of view or which are incomplete. It is then the aim of the Expert Group Review meeting planned on 19 October 2010 to allow the **judicial experts** to exchange their point of views on these specific issues identified during the revision of the comments so that a consensus and common understanding emerges on the **business and judicial level**. If necessary, the discussions on the more difficult points can be continued during the COPEN meeting on 20 October 2010, provided that the same Member State experts on legal aspects are still present. By then, the major business issues should have been solved and we should have a basis solid enough for continuing the work on the detailed technical specifications.

Please note that considering the calendar, bi-lateral discussions between Member States and the author of the "Business Analysis" can be envisaged between 11 October 2010 and 15 October 2010 in view of preparing the Expert Group Review meeting of 19 October 2010. In the very worst case where there would still be a lot of judicial matters unsolved, an additional workshop could still be envisaged after the COPEN meeting of 20 October 2010, probably around 26 October 2010 but this would already potentially delay the delivery of the *Detailed Technical Specifications* that is foreseen on 05 November 2010, thus potentially also delaying the COPEN meeting of 09 December 2010.

Personal Identification Data

During the "Inception Phase" it appeared that identification of persons based on the information exchanged between Member States is a major issue.

While it is not the aim of the *ECRIS Technical Specifications* to completely solve the identification difficulties, the *kinematics* of the ECRIS message exchanges should allow additional communications to take place between the Member States' central authorities so that the identities can be clarified in case of doubts.

The proposed approach is to foresee additional optional messages in the "Business Analysis" that focus on the identification problematic and provide electronic and structured ways for the central authorities to contact each other in view of clarifying identities. For example, if a central authority has identified several persons with the data that has been transmitted by the sender, the system could foresee that the central authority responds to the sender with the list of persons found and requests the sender to either provide additional information or to indicate which person is the right one.

Please note that for this topic, no specific questionnaire or workshop is currently foreseen. The proposals are part of the "Business Analysis" document which is to be reviewed by the Member States experts during the "Review Cycle" and, if necessary, further discussed during the "Expert Group Review meeting".

Additional Canonicalisation *of Data Elements*

In view of reducing the need for translation, the *ECRIS Technical Specifications* should provide as much as possible standardised elements as well as common and national reference tables.

The NJR project already defines a number of reference tables that have been established between the NJR partners.

In the context of the "Business Analysis", a part of the work needs to focus on the revision of these reference tables so as to align them with the ECRIS legal basis and to include also lists of values from the non-NJR Member States. It also needs to be evaluated if additional reference tables can be added, such as for example the most frequently used cities of each Member State, the most frequently used purposes for requests other than criminal proceedings, etc.

The proposed approach is to include the reference tables as an annex to the "Business Analysis" document which is to be reviewed by the Member States experts during the "Review Cycle" and, if necessary, further discussed during the "Expert Group Review meeting".

Logging and Monitoring

The "logging and monitoring" aspects have been extensively described earlier in this document since they are to be dealt with in a specific analysis.

The NJR project does not have a specific and well-defined approach for the logging and monitoring.

In view of identifying proposals, the proposed approach is the following:

- § iLICONN drafts a specific questionnaire on this subject.
- § The European Commission transmits the questionnaire to all Member States experts in view of collecting answers, using CIRCA.
- § Based on the answers received, iLICONN drafts proposals to be included in the "Logging, Monitoring and Statistics Analysis" document.

Statistics

In the NJR project, the statistics focus on counting the number of messages exchanged and comparing the figures between the partner States in order to identify discrepancies (for example Member State "A" indicates that it has sent 300 notifications to Member State "B" but Member State "B" indicates that it has only received 200 notifications from Member State "A").

In addition, the rejections of messages are also counted but without providing figures on the causes.

As defined by the ECRIS legal basis[47], the purpose of collecting statistical information is to report on the **efficiency** of the ECRIS data exchanges. However, since the ECRIS legal basis defines specific rules to be respected such as mandatory data elements or the usage of common categories for offences and sanctions, the report should also include statistics on these aspects.

[47] Council Decision 2009/316/JHA – Article 3, paragraph 7

The proposed approach for this analysis is the following:

- § iLICONN drafts a series of proposals based on the ECRIS legal basis and outcomes of the previous work on this project. Such proposals could for example include:
  - – Counting the number of times that each common offence and sanction category has been used. If some generic or open categories are frequently used, this can outline the need to revise one or more of the offence and penalties categories.
  - – Counting the number of times when a mandatory field ("mandatory" according to the ECRIS legal basis) has been filled with a blank or dummy value (such as for example a year of birth having the value "0000", an empty name or city, etc.).
- § The European Commission circulates these proposals to all Member States for revision, using CIRCA.
- § iLICONN consolidates the results of the revisions in the "Logging, Monitoring and Statistics Analysis" document.

If deemed necessary, the European Commission **may** organise **a workshop** in Brussels **with a limited and reduced number of experts** from the concerned Member States in order to reach a preliminary agreement.

Verification of Conformity

This subject has been extensively described earlier in this document since it is to be dealt with in the specific "Verification of Conformity Analysis".

It is to be noted that in NJR, as explained earlier in this document, a practical approach for testing and verification of conformity has been established.

The proposed approach for this analysis is the following:

- § iLICONN drafts a series of proposals based on the NJR experience and on the outcomes of the previous works on this project.
- § The European Commission transmits the proposals to all Member States experts in view of collecting feedback, using CIRCA.
- § iLICONN consolidates the results of the revisions in the "Verification of Conformity Analysis" document.

If deemed necessary, the European Commission **may** organise **a workshop** in Brussels **with a limited and reduced number of experts** from the concerned Member States in order to reach a preliminary agreement.

Impacts on ECRIS Technical Specifications

This section briefly outlines the priority to be given to of each theme described above. This is based on the potential impact of the outcomes of each theme on the definition of the *ECRIS Technical Specifications*.

Top Priority

The themes "Technical Architecture" and "Security of ECRIS Data Exchanges" are considered as requiring the highest priority in this project and need to be tackled first. Indeed, the solutions to be agreed on during the analyses on these topics have direct influence on the technical protocols, standards and formats to be used for all ECRIS data exchanges and must be taken into account in the definition of the detailed technical specifications.

In addition, the "Business Analysis" is also considered as requiring top priority due to the fact that it is essential to have first a clear definition of the ECRIS concepts (such as parameters, categories of purposes of requests, etc.), the domain model, the messages and the workflows. Indeed the "Business Analysis" must ensure that these elements are understood in the same way by all stakeholders.

High Priority

The topic "Electronic Exchange of Fingerprints" is also considered as requiring high priority since it can also influence, to some extent, the technical architecture to be defined for the ECRIS data exchanges. Indeed, in particular if the electronic fingerprint files are to be attached to the ECRIS messages in their binary form, a revision of the data exchange protocols to be used may be required. In particular, the technical limitations in terms of file formats, file sizes and time-outs need to be evaluated and defined.

Medium Priority

The following themes are considered as having medium priority, from a technical standpoint:

- "Logging and Monitoring"
- "Statistics"

While these topics are essential for the good functioning of the ECRIS data exchanges and in particular for their added value to the ECRIS end-users and for the Member States' central authorities, their impact on the definition of the *ECRIS Technical Specifications* is limited. Indeed, it is estimated that these will rather influence the detailed content of some specific XML messages rather than the whole technical architecture.

Low Priority

The topic "Verification of Conformity" is considered as having the lowest priority since it does not directly impact the definition of the *ECRIS Technical Specifications*.

Proposed Roadmap

The following detailed roadmap is proposed for dealing with the topics identified above in due time so as to not delay the final products of the *ECRIS Technical Specifications* project, using the proposed approaches.

Event	Date
Delivery of proposals on: - Technical Architecture - Security of Data Exchanges - Electronic Exchange of Fingerprints	10/09/2010
Feedback from Member States experts on: - Technical Architecture - Security of Data Exchanges - Electronic Exchange of Fingerprints	17/09/2010
Workshop in Brussels on: - Technical Architecture - Security of Data Exchanges	22/09/2010
Delivery: - Technical Architecture - Security Analysis - Business Analysis	27/09/2010

Delivery of questionnaire on "Logging and Monitoring" Delivery of proposals on "Statistics"	10/10/2010
Answers and feedback from Member States experts on "Logging and Monitoring" and on "Statistics"	20/10/2010
Workshop in Brussels on "Logging, Monitoring and Statistics" (only if necessary, to be confirmed after reception of feedback from Member States experts)	27/10/2010
Delivery: - Detailed Technical Specifications - ECRIS-NJR Fit-gap Analysis - Logging, Monitoring and Statistics Analysis	05/11/2010
Delivery of proposals on "Verification of Conformity"	10/11/2010
Feedback from Member States experts on "Verification of Conformity"	19/11/2010
Workshop in Brussels on "Verification of Conformity" (only if necessary, to be confirmed after reception of feedback from Member States experts)	29/11/2010
Delivery of "Verification of Conformity Analysis"	07/12/2010

Table 4 – Roadmap for Specific Themes

Please note that the Member States experts' collaboration will be requested heavily during the months of September, October and November 2010.

The roadmap proposed above takes into account the fact that, at the beginning of each month, a "Review Cycle" of the previous deliverables is planned.

As a result, a significant workload is to be expected for the Member States experts throughout each month, first providing comments on the products in the context of the "Review Cycle" defined earlier, then providing feedback and answers to the proposals and questionnaires for each specific theme.

ECRIS IMPLEMENTATION ROADMAP

This section provides a global overview of the proposed, indicative planning for the timely implementation of ECRIS in all Member States by April 2012:

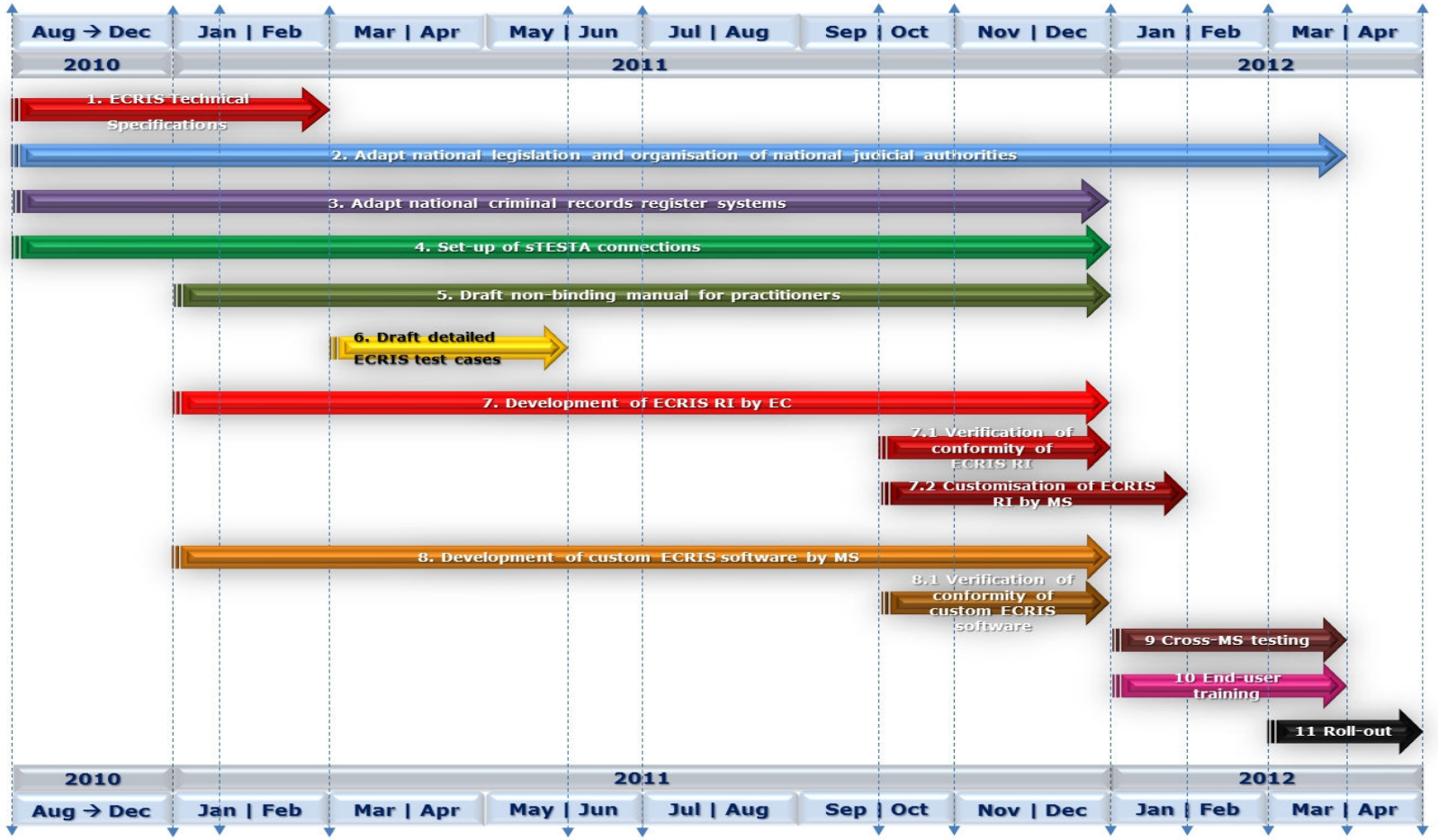

Figure 5 – ECRIS Implementation Roadmap

(1) Until 01/03/2011: Adoption of the *ECRIS Technical Specifications*

(2) From now until April 2012:

- The Member States adapt their national legislation so as to comply with the ECRIS legal basis (if necessary).
- The Member States adapt the organisation of their judicial authorities and working procedures so as to be able to operate ECRIS as defined in the legal basis (if necessary).

(3) From now until end of 2011:
The Member States' central authorities analyse and perform changes to the internal IT infrastructure; in particular changes to the criminal records register systems, in accordance with changes in their national legislation.

(4) From now until end of 2011:
All Member States' central authorities set-up and configure the sTESTA connections with all other Member States' central authorities and validate the connectivity.
(Please note that the NJR partners have indicated recurrently that the set-up of such sTESTA connections can be a lengthy process due to the high number of entities that need to intervene on a technical level so as to configure the network items such as routers, firewalls, switches, etc.)

(5) From Jan-2011 to end 2011: drafting of the non-binding manual for practitioners.

(6) From Mar-2011 to end of May-2011: definition of the detailed test cases for validating the ECRIS software implementations.

For the Member States using the *ECRIS Reference Implementation*:

(7) From Jan-2011 to end of 2011
Development of the *ECRIS Reference Implementation* by the European Commission:

- Jan-2011 and Feb-2011: procurement procedure (drafting of technical annex, evaluation of external contractors' offers, drafting and signature of contracts)
- From Feb-2011 to Sep-2011: analysis and implementation of *ECRIS Reference Implementation* software
  (In order not to delay the Member States intending to build an interface between the *ECRIS Reference Implementation* and their national criminal records register, the internal API of the *ECRIS Reference Implementation* must be defined and made available as early as possible.)

- Sep-2011: delivery to the concerned Member States' central authorities of the first version of the *ECRIS Reference Implementation* software for the customisation and integration into their IT infrastructure
- Oct-2011 to Dec-2011: unit and validation testing of the *ECRIS Reference Implementation* software
- (7.1) Oct-2011 to Dec-2011: in parallel to the validation testing, verification of the conformity of the *ECRIS Reference Implementation* software against the detailed technical specifications of ECRIS
- (7.2) Sep-2011 to Jan-2012: the concerned Member States' central authorities perform the installation and customisation of the *ECRIS Reference Implementation* software in order to integrate it into their IT infrastructure
- Dec-2011: delivery of the finalised and validated version of the *ECRIS Reference Implementation* software to the concerned Member States' central authorities

For the Member States upgrading their existing NJR software to the *ECRIS Technical Specifications* or developing a new custom ECRIS application:

(8) From Jan-2011 to end of 2011
- Analysis and implementation of the custom ECRIS application
- Unit and validation testing of the custom ECRIS application
- (8.1) Oct-2011 to Dec-2011: in parallel to the validation testing, verification of the conformity of the custom ECRIS application against the detailed technical specifications of ECRIS

For all Member States:

(9) From Jan-2012 to Mar-2012: testing between all Member States' ECRIS implementations; the preferred approach, which has also been used in the NJR project, is to perform intensive and in-depth testing with one or two Member States and then to proceed to light tests with the other Member States.

(10) From Jan-2012 to Mar-2012: training of the ECRIS end-users

(11) Mar- and Apr-2012: deployment of the ECRIS applications in the real production environments and effective start of the criminal records data exchanges between all Member States.

Risks

The following sub-chapters elaborate on the major risks that have been identified for the implementation of ECRIS.

ECRIS Technical Specifications

The following points are describing the major risks that have been identified specifically for the *ECRIS Technical Specifications* project.

Late Feedback from Member States Experts

Due to the tight schedule of the project, multiple tasks need to be performed in parallel and within short time periods. As a consequence, there is a risk for not receiving the feedback from all Member States experts in due time, potentially delaying the production of the main project artefacts.

Probability

The probability of occurrence of this risk is estimated to very high.

Indeed, due to the ambitious scheduling of the project and the fact that the Member States experts will be requested to provide feedback almost continuously in September, October and November 2010, it is almost certain that not all appointed Member States experts will be able to provide the necessary feedback to **all** deliverables of the *ECRIS Technical Specifications* project in due time.

Impact

The impact is estimated as low.

Indeed, it is not likely that iLICONN will not receive any feedback at all from Member States experts in due time for each deliverable. Thus, at least the feedback received can be consolidated into the deliverables in view of producing proposals in due time that can be deemed reasonable and acceptable for a majority of Member States.

Proposed Actions

The following actions are proposed for further reducing the impacts of this risk, depending on which feedback is received late:

- In the case where answers to questionnaires or feedback on early proposals is received late, then iLICONN can still base the project documents at first on the feedback received in due time by the Member States experts and on the proposals identified by the iLICONN staff during the analyses. The late answers and feedback of the remaining Member States experts can then be incorporated into the project documents **on a best effort basis** during the "Review Cycle".
- In the case where the "Review Cycle" comments are received late, then iLICONN and the European Commission will in any case already provide to all Member States experts their position on comments received in due time. iLICONN will still try to incorporate major comments that were delivered late, **based on a best effort basis**, into the project documents. However the remaining major comments will be left open for discussion during the Expert Group Review meetings and COPEN meetings.

Strongly Diverging Opinions

Due to the tight schedule, it might not be possible to find solutions in due time on all aspects of the project where the Member States' point of views are strongly diverging.

Probability

The probability of occurrence of this risk is estimated as high.

Indeed, if an issue is raised for which the opinions of the Member States' experts are strongly diverging, the schedule of the project does not leave much room for negotiating and finding alternatives or compromise solutions.

Impact

The impact is considered low.

Indeed, the issues that are potentially contentious are most likely not affecting the complete *ECRIS Technical Specifications* project but are rather related to specific aspects of the technical specifications, such as for example specific data elements in a given message or a validation rule to be applied to specific data elements. As a result, the impact would be that for such specific aspects of the *ECRIS Technical Specifications*, it would become difficult to establish a strict business rule or a rigid set of data elements in the messages to be exchanged between Member States.

Proposed Action

The following action is proposed for reducing the probability of occurrence and impact of this risk:

For each specific issue, the European Commission and iLICONN will provide if possible several proposals, with an indication of which solution is the preferred one. In the case that major disagreements appear in the comments received during the Review Cycle on the solution to be adopted (or in case of lacks of responses), the preferred solution is proposed in the first version of the main project deliverables by default and the other solutions listed as alternatives. The issue is then put on the agenda of the next Expert Group Review meeting and COPEN meeting if necessary in order to reach an agreement.

Late Changes to Project Products

Due to the tight schedule of the project, parallel works and overlapping between the project phases is foreseen. In particular, the formal approval of documents by the Expert Group and by the COPEN working party occurs for each document while the next deliverables have already been completed by iLICONN. Thus, changes that would be agreed upon only during the Expert Group Review meeting or even COPEN meeting cannot be taken into account in the next project products. Updating the project products later than expected may potentially delay their adoption by the Member States experts and COPEN Working Party.

Probability

The probability of occurrence is considered low.

Indeed, the probability of occurrence is already reduced by the fact that all deliverables produced by iLICONN are submitted to the Member States experts for revision as a first step of the "Review Cycle". This gives the Member States experts the possibility to already express their views on the proposed solutions sufficiently early during the "Review Cycle" and before the next products have been finalised.

Furthermore, for specific topics that have been identified earlier in this document, additional steps are proposed for collecting sufficient feedback from the Member States experts before drafting the project products, so as to ensure that the solutions proposed by iLICONN can satisfy the needs of the Member States to the best possible extent.

Impact

The impact of such changes that would be agreed upon late in the "Review Cycle" depends on the nature of the changes and on how late these are agreed upon.

The overall impact is considered moderate.

Minor changes that relate for example to a specific data element in a given message can easily be added into the project products after they have been finalised. It would only require that the updated document is again circulated to all Member States experts for formal approval of the change.

Major changes are highly unlikely to occur so late in the "Review Cycle". Should such a major change however occur, it would require at worst iLICONN to completely rework one of the project products, thus delaying its adoption by the Member States and thus the overall project.

Proposed Actions

It is to be noted that the approach proposed in this document for the *ECRIS Technical Specifications* project is already reducing the probability of occurrence and potential impact of this risk.

Indeed, the project has been divided into phases and foresees distinct products, each with a limited and well-defined scope. Thus, at worst, if a late major change should appear, only a limited part of the *ECRIS Technical Specifications* would require a major revision.

Misunderstanding of ECRIS Technical Specifications

Due to different national legislations and different penal codes of the Member States, as well as different languages and backgrounds of the involved persons, there is a risk of misunderstanding each other and misinterpreting the information provided in the *ECRIS Technical Specification* deliverables.

Probability

The probability of occurrence is considered low.

Indeed, the probability is already reduced by the following factors:

- The ECRIS legal basis and the NJR project provide already a common basis and context understood by all actors.
- English is systematically used as working language, especially in the field of information technology.

- Several experts are appointed in each Member State.
- The *ECRIS Technical Specifications* project features a "Glossary" that helps clarifying specific terms and abbreviations.
- The *ECRIS Technical Specifications* project foresees several products that provide analyses on the data exchanges from different angles, both functional and technical. This helps aligning the understanding of the functional aspects of the data exchanges for the IT experts and gives an insight in the technical matters to the legal and functional experts.
- All documents produced by iLICONN undergo an internal revision by several persons before being delivered to the Member States experts. At this stage, major ambiguities are already detected and corrected.

Impact

The impact of this risk is considered low.

Indeed, a misunderstanding or misinterpretation can only affect the *ECRIS Technical Specifications* project if it results in Member States not agreeing on proposed solutions. In such cases, the diverging opinions are brought forward in the Expert Group Review meetings or COPEN meetings where the actors have the opportunity to clarify the matters and align their understanding.

Proposed Action

The probability of occurrence can be further reduced, if deemed necessary, by the Member States' central authorities by translating the documents produced by iLICONN (questionnaires, meeting minutes, analysis documents, etc.) into one of their official languages.

Overall ECRIS Implementation

The following sub-chapters elaborate on the major risks that have been identified for the overall implementation of ECRIS, after the finalisation and adoption of the *ECRIS Technical Specifications* project.

Late Adaptation of National Regulations

It appears that, in order to implement ECRIS, many Member States need to adapt their national legislation. In most cases, this is due to the obligations defined in the ECRIS legal basis to store and retransmit a well-defined set of specific information on criminal records or to process requests for purposes other than criminal proceedings.

There is a risk that in some Member States the changes to the national legislation are not applied before April 2012, resulting in these Member States to not comply with at least a part of the provisions of the ECRIS legal basis.
(Please note that in the answers to the "Inception Phase Questionnaire", no major issues have been identified regarding severe legal incompatibilities between national laws and the implementation of the ECRIS legal basis so far. This risk is thus considered very low at this stage.)

Probability

Based on the answers provided so far to the "Inception Phase Questionnaire", the probability of occurrence of this risk is considered as moderate.
Indeed, the Member States having replied in due time to the questionnaire have already identified the changes to be brought to their national legislation and have already launched the procedures for adapting it. For the Member States that did not yet reply to the questionnaire, the current state is unknown.

Impact

The impact is considered as low.
Indeed, the previous regulations and European decisions were already setting several years ago the legal ground for allowing the effective exchanges of information on criminal records between the Member States. As such, the national legislation of all Member States is already to some extent allowing the information exchanges described in ECRIS. As a result, the non-compliance would only relate to very specific obligations defined in the ECRIS legal basis but not to the information exchange as a whole. Furthermore, known difficult issues such as the possible exchange of fingerprints or of specific identification numbers have been defined on purpose as optional in the ECRIS legal basis so as to avoid major incompatibilities with the national legislation of several Member States.

Possible Actions

The *ECRIS Technical Specifications* project will already help raise awareness on specific aspects of ECRIS that need to be implemented and that may have legal impacts in some Member States.

This will already allow the Member States to launch the necessary procedures for adapting their national legislation.

Late Adoption of ECRIS Technical Specifications

There is a risk that the *ECRIS Technical Specifications* are adopted later than expected. This would reduce the time available for the Member States' central authorities for developing the ECRIS software and could in turn delay the whole implementation of the ECRIS legal basis for some Member States.

Probability

The overall probability of occurrence of this risk is considered moderate, based on the risks analysed and assessed in the previous chapter.

Please note that the overall roadmap proposed earlier in this document also aims at reducing the probability of occurrence of this risk. Indeed, it proposes to already perform some tasks before or in parallel of the actual implementation of the ECRIS software, such as for example setting up sTESTA connections, implementing changes in own IT infrastructure, etc.

Impact

The overall impact is considered moderate, but obviously depends on how late the adoption of the *ECRIS Technical Specifications* will occur.

The Member States being partners in the NJR project and having already developed appropriate NJR software are already currently realising a part of the data exchanges defined in the ECRIS legal basis. These Member States mainly need to adapt their systems in order to comply with the changes that will be defined in the *ECRIS Technical Specifications*, which is less difficult and less time-consuming than starting from scratch.

Furthermore, due to the decentralised nature of ECRIS, even if specific Member States cannot perform exchanges of information on criminal records with the other Member States in due time, the latter are not blocked and can already exchange data with the operational Member States' central authorities.

Possible Actions

The impact and probability of occurrence of this risk can be further reduced by actually starting the developments before the *ECRIS Technical Specifications* are adopted, focusing on the parts that do not directly perform the data exchanges such as for example end-user interfaces, internal interfaces towards the criminal records register, internal workflows to be used by the central authorities, etc.

Delay in Changes to National Criminal Records Register

In order for the ECRIS data exchanges to be operational, most Member States need to adapt their national criminal records register and supporting IT infrastructure. Delays in these tasks can potentially also delay the effective start of the ECRIS data exchanges with other Member States' central authorities.

Probability

Based on the answers provided so far to the "Inception Phase Questionnaire", the probability of occurrence of this risk is considered as moderate.

Indeed, the Member States having replied in due time to the questionnaire have already identified the changes to be brought to their national criminal records and supporting IT infrastructure and most have already launched the procedures for making the necessary changes. For the Member States that did not yet reply to the questionnaire, the current state is however unknown.

In addition, most of the Member States being partners in the NJR project, and having already developed appropriate NJR software, have already realised changes to their criminal records registers and to their IT infrastructure in order to be able to operate NJR properly. For these Member States, the amount of changes to still be performed for complying with ECRIS is fairly limited. Furthermore, some Member States have already recently modernised their IT infrastructure (or are currently in the process of doing so) and have taken into account to some extent the exchanges of information with other Member States.

Impact

Based on the answers provided so far to the "Inception Phase Questionnaire", the impact of this risk is considered moderate.

Indeed, due to the decentralised nature of ECRIS, even if specific Member States cannot perform exchanges of information on criminal records with the other Member States in due time, the latter are not blocked and can already exchange data with the operational Member States' central authorities.

Possible Actions

The following mitigation actions are proposed for reducing the impact and probability of occurrence of this risk:

- A possible action is to design the ECRIS software as an application that can be operated independently from the criminal records register, featuring for example a complete user interface, even if it is integrated to the criminal records register IT system. In this way, even if the changes to the criminal records register are delayed, the ECRIS application can be operated directly by the personnel of the central authority and the ECRIS data exchanges can be performed effectively.
- Using the *ECRIS Reference Implementation* until the national IT infrastructure is ready is also a possible action for reducing the dependency on the criminal records register.

Late Availability of ECRIS Reference Implementation

Some Member States have marked their intention to use whole or part of the *ECRIS Reference Implementation* for realising the ECRIS data exchanges with other Member States. Delays in the availability of the *ECRIS Reference Implementation* could delay the effective start of the ECRIS data exchanges with other Member States' central authorities.

Probability

Based on the feedback provided during the "Inception Phase", the probability of occurrence of this risk is considered as moderate.

Indeed, on one hand, the European Commission has gained significant working experience in this specific area through the development of the *NJR Reference Implementation*.

On the other hand, the remaining time available for the development of the *ECRIS Reference Implementation* is fairly short according to the roadmap descried earlier in this document.

Impact

Based on the answers provided so far to the "Inception Phase Questionnaire", the impact of this risk is considered as moderate.

Indeed, most of the Member States being partners in the NJR project, and having already developed custom NJR software, have already marked their intention to further develop their custom software rather than using the *ECRIS Reference Implementation*.

Possible Actions

The following mitigation actions are proposed for reducing the impact and probability of occurrence of this risk:

- Shortening the procurement process by using preferably one of the external contractors that has been awarded the framework contract applicable in 2011.
- Retaining as much as possible staff, external and internal, having proven experience in the specific fields of expertise required in ECRIS (i.e. exchange of information on criminal records, data exchanges through web services, NJR experience, etc.)
- Starting the *ECRIS Reference Implementation* development project as soon as possible.
- Performing a close and frequent monitoring of the progress of the developments.
- Reducing if necessary the scope of the *ECRIS Reference Implementation* development project to a minimum in order to avoid delays.
- Providing as early as possible the internal API of the *ECRIS Reference Implementation* in order not to delay the Member States intending to build an interface between the *ECRIS Reference Implementation* and their national criminal records register
- Keeping the ECRIS technical specifications as close as possible to the current NJR technical specifications

Late Availability of Non-Binding Manual for Practitioners

The ECRIS legal basis foresees the drafting of a non-binding manual for practitioners that will address the procedures governing the exchange of information, in particular the modalities of identification of offenders, common understanding of the categories of offences and penalties and measures, and explanation of problematic national offences and penalties and measures, and ensuring the coordination necessary for the proper operation of ECRIS.

Late availability of this manual could potentially delay the effective start of the ECRIS data exchanges between Member States' central authorities.

Probability

The probability of occurrence of this risk cannot be precisely assessed at this stage and is thus assumed to be moderate. Indeed, it is most likely that a first version of this manual will be ready in due time but that it might not yet clarify all aspects of the ECRIS data exchanges or not yet provide guidelines for all specific situations.

Impact

The consequence of this risk is considered low since the unavailability of the non-binding manual for practitioners would not block the usage and operation of the ECRIS software. It would only render it more difficult from an end-user's point of view and maybe reduce the efficiency of the ECRIS data exchanges.

Possible Actions

The following mitigation actions are proposed for reducing the impact and probability of occurrence of this risk:

- Documenting the *ECRIS Technical Specifications* as clearly as possible, illustrating the various cases with concrete and realistic examples.
- Defining clear and complete use cases in the *ECRIS Reference Implementation* development project and publishing them.
- Translating and providing the relevant documents of the *ECRIS Technical Specifications* and of the *ECRIS Reference Implementation* development project to the ECRIS end-users.
- During the ECRIS end-user trainings, focus on the most common specific situations and issues that are likely to be encountered in the daily operation of ECRIS and illustrate them with concrete examples.

Delay in Development of Custom ECRIS Software

Some Member States have marked their intention to either upgrade their existing NJR software or to develop new custom ECRIS software rather than using the future *ECRIS Reference Implementation.* Delays in the developments of these custom ECRIS applications could delay the effective start of the ECRIS data exchanges with other Member States' central authorities.

Probability

Based on the answers provided so far to the "Inception Phase Questionnaire", the probability of occurrence of this risk is considered as moderate.

Indeed, the Member States having developed their own NJR application and foreseeing to upgrade it for complying with the *ECRIS Technical Specifications* have already gained significant expertise that can be reused. In particular, this will allow these Member States to avoid pitfalls of such custom developments. Most of these Member States also do not need to undergo a lengthy procurement procedure such as for example a public call for tender since they are either already contracting with specific external providers or performing the developments by in-house internal staff.

For the Member States that did not yet reply to the questionnaire, that are not NJR partners and that are foreseeing to develop their own custom ECRIS software, the probability of occurrence of this risk remains unknown.

Impact

The impact of this risk is considered as moderate.

Indeed, the Member States having already developed custom NJR software are already currently realising a part of the data exchanges defined in the ECRIS legal basis. These Member States mainly need to adapt their systems in order to comply with the changes that will be defined in the *ECRIS Technical Specifications*, which is less difficult and less time-consuming than starting from scratch.

Furthermore, due to the decentralised nature of ECRIS, even if specific Member States cannot perform exchanges of information on criminal records with the other Member States in due time, the latter are not blocked and can already exchange data with the operational Member States' central authorities.

Possible Actions

The following mitigation actions are proposed for reducing the impact and probability of occurrence of this risk:

- The *ECRIS Reference Implementation* should be developed as a modular software system, so that Member States have the option to reuse selected parts of this system for building their own custom software (such as for example the part of the software that handles the *web services* communications with other Member States' ECRIS applications). Each such module of the *ECRIS Reference Implementation* should thus feature a technical interface that allows easily integrating it with Member States IT tools.
- The probability of occurrence can be reduced by sharing the Member States' expertise with each other, following for example the coaching approach that has been already used in the NJR project.
- The probability of occurrence can be reduced for the current NJR partners by keeping the *ECRIS Technical Specifications* as close as possible to the current NJR technical specifications, minimising thus the number of changes that they will need to implement for upgrading their current NJR application.

Future Changes in ECRIS Technical Specification

The main outcomes of this project are the *ECRIS Technical Specifications* that will serve as basis for the development of the ECRIS applications. However, later judicial and technical workgroups may identify the need for bringing changes to these technical specifications before April 2012. This could delay the effective start of the ECRIS data exchanges between the Member States' central authorities.

Probability and impact of this risk cannot be assessed at this stage since they mainly depend on (1) the completeness and level of maturity of the *ECRIS Technical Specifications* and on (2) the nature and the complexity of the changes to be agreed upon in these workgroups.

At this stage, it can only be noted that the next NJR Technical Workgroup meetings should, with the support of the NJR Judicial Workgroup, focus on bringing the NJR specifications v1.5 as close as possible to the *ECRIS Technical Specifications* and, in doing so, if possible avoid major changes to the *ECRIS Technical Specifications*.

(sTESTA) Connectivity Issues

The ECRIS data exchanges will take place on the sTESTA communication network. Unavailability or temporary disruptions of the networks used – both sTESTA and the national networks – would prevent the Member States' ECRIS applications from effectively communicating with each other.

The probability of occurrence of this risk is low. Indeed, sTESTA is a proven network used for many other data exchanges between Member States' administrations and features a very high availability of 99,8%. Similarly, the national networks used within the Member States are highly available and robust networks specifically designed for transferring large amounts of data between national administrative authorities.

Due to the nature of ECRIS, the impact is limited to temporary disruptions of connectivity between two Member States' central authorities. While such disruptions are certainly annoying, they do not represent a major problem for complying with the ECRIS legal basis.

In order to reduce delays in the set-up of the sTESTA connections, the following actions are proposed:

- As indicated in the roadmap described earlier in this document, setting up the sTESTA connections right away is recommended. It is indeed not necessary to wait for the *ECRIS Technical Specifications* or for the ECRIS applications to be finalised.
- Assistance from the European Commission and from the NJR partners can be requested in order to benefit from the available experience.

Technical Limitations for Implementing ECRIS Technical Specifications

The *ECRIS Technical Specifications* will serve as a basis for the development of all ECRIS applications. There is a risk that the technical solutions adopted in these technical specifications cannot be implemented in due time on specific IT infrastructures or development platforms of Member States due to technical incompatibilities or limitations.

The probability of occurrence of this risk is considered as very low. Indeed, the preferred choices of using *web services* and XML are already oriented towards a maximum compatibility with all types of IT infrastructures, programming languages, software development technologies and tools. These standards are currently widely used, well-supported and have proven through the NJR project to be fairly straightforward to use and to implement.

The impact of this risk is also considered very low. Since *web services* and XML are both text-based protocols, it is in any case possible to develop ad-hoc support in all types of programming languages and development platforms. The only risk here is actually that a specific development platform used by a Member State does not provide native out-of-the-box support for whole or parts of these standards, in which case the Member State must perform additional custom developments in order to "manually" implement the parsing and processing of the *web services* messages.
It is possible to avoid this risk altogether by using whole or parts of the *ECRIS Reference Implementation*.

Risk Matrix

The following sections summarise the risks defined previously in form of risk matrixes, defining for each the risk exposure that is obtained by combining the probability of occurrence of the risk with its potential impact.
The risk exposure is a value attributed to the risk for the purposes of comparing the importance of the risks and it is calculated as follows: risk exposure = probability x impact.
In view of calculating the risk exposure, numeric values are assigned to the risk probability and impact as follows:

- High → associated numeric value = 3
- Medium → associated numeric value = 2
- Low → associated numeric value = 1

The risk exposure is rated as follows:

- High if higher or equal to 5
- Medium if 3 or 4
- Low if 1 or 2

Probability / Impact	L(1)	M(2)	H(3)
L(1)	L (1)	L (2)	M (3)
M(2)	L (2)	M (4)	H (6)
H(3)	M (3)	H (6)	H (9)

Table 5 – Risk exposure table

Matrix for ECRIS Technical Specifications *Project*

The following matrix summarises the major risks that have been identified specifically for the *ECRIS Technical Specifications* project.

ID	NAME	PROBABILITY	IMPACT	EXPOSURE
RTS-01	Late Feedback from Member States Experts	3	1	3
RTS-02	Strongly Diverging Opinions	3	1	3
RTS-03	Late Changes to Project Products	1	2	2
RTS-04	Misunderstanding of ECRIS Technical Specifications	1	1	1

Table 6 – Risk matrix for *ECRIS Technical Specifications* project

Matrix for Overall ECRIS Implementation

The following matrix summarises the major risks that have been identified for the overall implementation of ECRIS.

ID	NAME	PROBABILITY	IMPACT	EXPOSURE
ROE-01	Late Adoption of ECRIS Technical Specifications	2	2	4
ROE-02	Delay in Changes to National Criminal Records Register	2	2	4
ROE-03	Late Availability of ECRIS Reference Implementation	2	2	4
ROE-04	Delay in Development of Custom ECRIS Software	2	2	4
ROE-05	Late Adaptation of National Regulations	2	1	2
ROE-06	Late Availability of Non-Binding Manual for Practitioners	2	1	2
ROE-07	(sTESTA) Connectivity Issues	1	1	1
ROE-08	Future Changes in ECRIS Technical Specification	?	?	?

Table 7 – Risk matrix for *ECRIS Technical Specifications* project

ANNEX – Overview of Member States Answers

The following sub-chapters provide a view on answers provided by the Member States' central authorities to specific questions of the "Inception Phase Questionnaire" and which have been taken into account for drafting major elements of this document.

General

§ Member States having **one single entity** that will operate the ECRIS software:
  – Having one national central authority managing criminal records:
    AT, BE, CZ, DE, EE, ES, FI, FR, HU, LT, LU, NL, PL, PT, RO, SE, SI, SK, UK[1]
  – Having multiple authorities handling exchanges of criminal record information with other Member States: /

§ Member States planning changes to their national legislation in order to implement ECRIS:
  – Requiring **significant** legal changes:
    AT, CZ, DE, EE, FR, LT, PL, RO, SK
  – Requiring legal changes: FI, HU, NL, PT, SE
  – Not requiring legal changes: BE, ES, UK
  – Unknown: LU, SI

§ Member States planning major changes to their criminal records register and/or IT infrastructure until April 2012:
  – Planning **significant** changes:
    AT, BE, EE, FI, LT, RO, UK
  – Planning changes: FR, LU, NL, PL, SE
  – Not planning changes: CZ, DE, ES, HU, SI, SK
  – Unknown: PT

§ Member States' plans for implementing ECRIS software:
  – Will use whole or parts of the *ECRIS Reference Implementation*:
    AT (maybe), BE, CZ, EE, NL, RO, SE
  – Will develop custom ECRIS software: DE, FI, HU, LU, PL, SK
  – Have not yet decided: ES, FR, LT, PT, SI, UK

Centralised Coordination and Management

§ Centralisation of the storage, publication and maintenance (i.e. regular updating) of the ECRIS technical specifications and related documentation:

[1] Please note that UK has one central authority acting as interface towards the other Member States but internally manages three distinct national criminal records registers.

- In favour of centralisation: AT, BE, DE, FI, FR, HU, LT, LU, NL, PL, RO, SK, UK
- Prefer to keep on national level: SI
- Both centralised and national levels together: CZ, SE
- Unknown: EE, ES, PT

§ Centralisation of support and helpdesk functions:
- In favour of centralisation: BE, FR, HU, LT,LU,NL,SK,UK
- Prefer to keep on national level: AT, PL
- Should be shared between central and national level: CZ, DE, FI, RO, SE, SI
- Unknown: EE, ES, PT

§ Centralisation of point of contact and coordination for trouble-shooting:
- In favour of centralisation: BE, FR, HU, LT, LU, RO, SK, UK
- Prefer to keep on national level: AT, NL, PL
- Should be shared between central and national level: CZ, DE, FI, SE, SI
- Unknown: EE, ES, PT

§ Centralisation of point of contact for sTESTA matters:
- In favour of centralisation: ES, FI, HU, LT, LU, NL, PL, RO, SI, UK
- Prefer to keep on national level: AT
- Should be shared between central and national level: CZ, DE, SE, SK
- Unknown: BE, EE, FR, PT

§ Centralised coordination of activities related to release and versioning management:
- In favour of centralisation: BE, DE, FI, FR, HU, LT, LU, NL, RO, SK, UK
- Prefer to keep on national level: /
- Should be shared between central and national level: AT, CZ, SE, SI, PL
- Unknown: EE, ES, PT

§ Centralised communication and follow-up on progress of activities:
- In favour of centralisation: AT, BE, DE, FI, FR, HU, LT, LU, NL, PL, SK, UK
- Prefer to keep on national level: /
- Should be shared between central and national level: CZ, RO, SE
- Unknown: EE, ES, PT, SI

- Centralised coordination and organisation of judicial and technical workgroups:
  - In favour of centralisation: AT, BE, DE, FI, FR, HU, LT, LU, NL, PL, RO, SK, UK
  - Prefer to keep on national level: /
  - Should be shared between central and national level: CZ, SE, SI
  - Unknown: EE, ES, PT
- Centralised verification of conformity of national ECRIS applications against *ECRIS Technical Specifications*:
  - In favour of centralisation: BE, HU, LT, PL, RO, SK, UK
  - Prefer to keep on national level: AT, DE, FI, FR, LU, NL
  - Should be shared between central and national level: CZ, SE, SI
  - Unknown: EE, ES, PT

Assumptions

- Considers acceptable that the sending Member State should transmit the data in one of its own official languages and that it is the responsibility of the receiving Member State to perform the necessary translation/transliteration:
  - Yes: CZ, DE, ES, FR, LT, LU, NL, PL, SK, UK
  - No: AT, BE, FI, HU, RO, SE
  - Unknown: EE, PT, SI
- On the level of security of the data exchanges, is considering the NJR security principles sufficient also for the ECRIS data exchanges:
  - Yes: BE, CZ, DE, EE, ES, FR, LT, LU, PL, SK, UK
  - No: NL
  - Unknown: AT, FI, HU, PT, RO, SE, SI
- Are supporting the usage of web services, XML and UTF-8 for implementing the computerised data exchanges between ECRIS applications:
  - Yes: AT, CZ, BE, DE, EE, ES, FI, FR, HU, LT, LU, NL, PL, RO, SE, SI, SK, UK
  - No: /
  - Unknown: PT
- Is interested in sending electronic fingerprints data in the ECRIS data exchanges as from April 2012 onwards:
  - Yes: LT, RO, UK
  - Maybe: SE
  - No: AT, CZ, BE, DE, EE, ES, FI, FR, LU, NL, PL, PT, SI, SK
  - Unknown: HU