WAVESTONE

Feasibility study and cost assessment of the establishment of a centralised ECRIS TCN solution

June 13, 2017

V5.00 – Final Version

This study was carried out for the European Commission Directorate-General for Justice and Consumers by Wavestone.

Authors

Débora Di Giacomo

Stefan Georgiev

Ludovic Colacino Dias

Reviewers

Dick Heimans

Jaime Lopez-Loosvelt

Haryo Nindito

Disclaimer

The information and views set out in this study are those of the author(s) and do not necessarily reflect the official opinion of the European Commission. This study has been carried out for information and consultation purposes only. It has not been adopted and should not be regarded as representative of the views of Commission staff. It does not in any way prejudge, or constitute the announcement of, any position on the part of the Commission on the issues covered. The European Commission does not guarantee the accuracy of the information provided, nor does it accept responsibility for any use made thereof. The cost information presented in this study are rough estimates and do not represent any firm commitment. Neither the European Commission nor any person acting on the European Commission’s behalf may be held responsible for the use which may be made of the information contained therein.

Table of Contents

List of Tables

List of Figures

Revision History

Date	Version	Description	Author(s)	Reviewed by
19.01.2017	0.01	Definitions of the table of contents and document structure	Débora DI GIACOMO	Jaime LOPEZ LOOSVELT Haryo NINDITO
03.03.2017	0.02	Updated table of contents	Débora DI GIACOMO	Jaime LOPEZ LOOSVELT Haryo NINDITO
10.04.2017	0.08	Adding sections "Description of ECRIS TCN system". Version submitted to the client for high level review.	Débora DI GIACOMO Stefan GEORGIEV Ludovic COLACINO DIAS	Dick HEIMANS Jaime LOPEZ LOOSVELT Haryo NINDITO
02.05.2017	0.17	Internal review and development of the study.	Débora DI GIACOMO Stefan GEORGIEV Ludovic COLACINO DIAS	Débora DI GIACOMO
08.05.2017	1.00	Draft version delivered for client's review.	Débora DI GIACOMO Stefan GEORGIEV Ludovic COLACINO DIAS	Dick HEIMANS Jaime LOPEZ LOOSVELT Haryo NINDITO
29.05.2017	2.00	Updated version delivered for client's review.	Débora DI GIACOMO Stefan GEORGIEV Ludovic COLACINO DIAS	Dick HEIMANS Jaime LOPEZ LOOSVELT Haryo NINDITO
01.06.2017	2.01	Implementation of comments following client's review.	Débora DI GIACOMO Stefan GEORGIEV Ludovic COLACINO DIAS	Débora DI GIACOMO
06.06.2017	3.00	Final version delivered for client's review.	Débora DI GIACOMO Stefan GEORGIEV Ludovic COLACINO DIAS	Dick HEIMANS Jaime LOPEZ LOOSVELT Haryo NINDITO
12.06.2017	4.00	Implementation of comments following client's review.	Débora DI GIACOMO Stefan GEORGIEV Ludovic COLACINO DIAS	Dick HEIMANS Jaime LOPEZ LOOSVELT Haryo NINDITO
13.06.2017	5.00	Delivery of final version for client's acceptance.	Débora DI GIACOMO Stefan GEORGIEV Ludovic COLACINO DIAS	Dick HEIMANS Jaime LOPEZ LOOSVELT Haryo NINDITO

Executive summary

The European Criminal Record Information System (ECRIS) was established in April 2012[1] to make the exchange of information on criminal convictions among Member States[2] efficient. The purpose of ECRIS is to ensure that all previous convictions handed down in other Member States can be taken into account at the time of a new conviction, or for other purposes, as defined by national law. The system works effectively for EU nationals given that the nationality of an EU national is considered to be the 'reference' Member State nationality. Regarding Third Country Nationals and Stateless persons (TCN)[3], Member States do not know which Member State to contact with requests for criminal record information, thus resulting in either blanket requests or in no exchanges of information.

Against this background, on 19 January 2016, the European Commission adopted a proposal[4] for a Directive amending Council Framework Decision 2009/315/JHA[18], regarding ECRIS and TCN, and replacing Council Decision 2009/316/JHA[17]. The proposal envisages the establishment of a mechanism where Member States could easily identify in which Member State(s) TCN have already been convicted so that the criminal record information request can be addressed to the correct Member State. This mechanism is hereafter called the ECRIS TCN solution. Furthermore, the proposal foresees the inclusion of fingerprints for the purpose of ECRIS TCN exchanges.

In order to support the European Commission on the legislative process for the establishment of the ECRIS TCN solution, feasibility studies and cost assessments were conducted in 2015[5] and 2016[6]. Among various options to implement the ECRIS TCN solution, the studies indicated that a centralised system for storing alphanumeric and fingerprint identity data would be the favourite option for the implementation of the ECRIS TCN solution.

In this context, the European Commission Directorate-General for Justice and Consumers (DG JUST) mandated WAVESTONE to further assess the technical feasibility and cost impacts of implementing a centralised ECRIS TCN solution as well as to analyse the interoperability, future-proofing[7], and possible extensions of the foreseen system.

[1] 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.

[2] 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.

[3] TCN is any person who is not a citizen of the European Union within the meaning of Art. 20(1) of TFEU and who is not a person enjoying the Union right to free movement, as defined in Art. 2(5) of the Schengen Borders Code. In this context the term TCN comprises also stateless persons.

[4] Proposal for a Directive of The European Parliament and of The Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, 19 January, Brussels.

[5] Information Communication Technology (ICT) Final Report, Assessment of ICT impacts of the legislative proposal for ECRIS TCN system regarding the exchange of convictions for third country nationals and stateless people (TCN), Kurt Salmon, Brussels, 4 December 2015.

[6] Final Report, Feasibility study on the inclusion of pseudonymised fingerprints in ECRIS TCN exchanges, Kurt Salmon, Intrasoft, GLSI, Brussels, 30 June 2016.

[7] In the context of this study, 'future-proofing' is a process of designing a software/computer system, in a way that it can still be used in the future, even when technology changes.

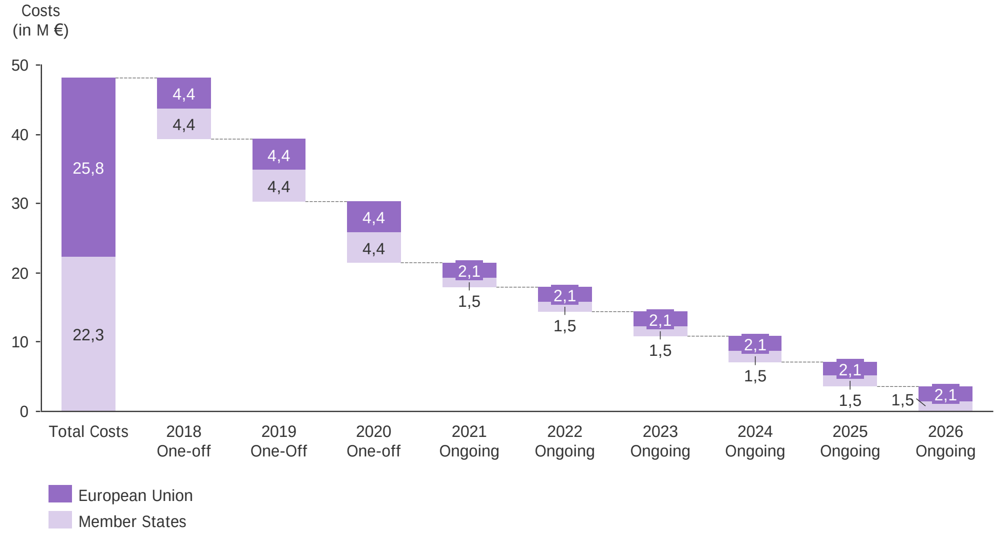
This study follows the Better Regulation Guidelines[8] and it is supported by the ISA method[9]. As a direct input is used the data collected in the scope of the two cost assessments conducted consequently in 2015[10] and 2016[11] as well as data gathered during dedicated interviews conducted in 2017 with eu-LISA and specialised AFIS and search engine vendors[12].

This study detailed the high level architecture, key principles and processes of the envisaged centralised ECRIS TCN solution. The proposed centralised ECRIS TCN solution addresses the current two main challenges of ECRIS:

- (i) the inefficiency in the ECRIS exchanges regarding TCN, by enabling 'hit/no hit' searches identifying the Member State(s) holding previous convictions of a TCN, and
- (ii) the issues on the identification of the specific convicted person by including fingerprints as identifier of a convicted person.

Technically, the solution focuses on fulfilling the current requirements of ECRIS, specifically with regard to availability, response time and storage capacity. In this context the cost impact of implementing a centralised ECRIS TCN solution is approximately EUR 48 million, EUR 26 million incurred by the European Union and EUR 22 million incurred by the Member States. Figure 1 below shows the breakdown of the incurred costs over three years of implementation (i.e. one-off costs) and the first six years of system operations (i.e. ongoing costs).

Figure 1 Centralised ECRIS TCN solution: Total costs summary



Source: WAVESTONE Data Analysis, March 2017.

Additionally, inspired by the Commission's communication 'Stronger and Smarter Information Systems for Borders and Security[13] and requested by the European Commission, this study also investigates

[8] Better Regulation Guidelines [COM (2015)205 final] European Commission, 19.05.2015

[9] The ISA Method for Assessing ICT Implications of EU Legislation is applied to the assessment of impacts approach (method not yet published).

[10] Information Communication Technology (ICT) Final Report, Assessment of ICT impacts of the legislative proposal for ECRIS TCN system regarding the exchange of convictions for third country nationals and stateless people (TCN), Kurt Salmon, Brussels, 4 December 2015.

[11] Final Report, Feasibility study on the inclusion of pseudonymised fingerprints in ECRIS TCN exchanges, Kurt Salmon, Intrasoft, GLSI, Brussels, 30 June 2016.

[12] Private enterprises specialised in security and identity solutions with experience in biometric matching technologies.

[13] Communication from the Commission to the European Parliament and the Council, Stronger and Smarter Information Systems for Borders and Security, COM(2016) 205 final, Brussels, 6.4.2016.

the feasibility and cost impacts of ensuring the interoperability, future-proofing, and extensions of the foreseen system. These are important aspects to be considered in the decision making process of the European Commission which would address needs beyond the ones currently highlighted by the ECRIS community. These aspects would enable the use of the ECRIS-TCN system by a broader audience and extend its initial scope and features.

The integration of the centralised ECRIS TCN solution with other European large scale systems would facilitate the access of data on convicted persons to other stakeholders beyond the justice domain (e.g. migration, home affairs, border control, etc.).

While this integration is technically feasible, it entails functional, operational and legal impacts, given that data exchanges between the centralised ECRIS TCN solution and any other large scale system impact need to be clearly identified and regulated by European and national legislations. This would also add administrative burdens on the ECRIS Central Authorities that would need to respond to new requesting authorities and for different purposes than those foreseen by the current ECRIS. Technically, the integration of the central ECRIS TCN system with large scale systems such as the ones used in the immigration and border control domains (e.g. SIS II[14], ETIAS[15], EES[16]) would require that the central ECRIS TCN system complies with significantly higher requirements on availability (99.99% instead of 97%) and target response time (real-time instead of up to one hour). This study estimated that a highly available central ECRIS TCN system would costs approximately EUR 15 million more than a central ECRIS TCN system for a nine-year period; accounting EUR 6,6 million one-off costs for the system implementation and EUR 1,4 million yearly ongoing costs for the system operation. This additional cost is mostly related to the need to update the IT infrastructure, the central component for monitoring and analytics, the central AFIS system component and the central alphanumeric search engine to comply with the high availability requirements.

This study also investigated the possibility of using a shared Biometric Matching Services (BMS) for the central ECRIS TCN system rather than setting up a dedicated central AFIS component. Similar to the integration with other EU large scale systems, integrating the centralised ECRIS TCN solution with the shared BMS would require national and EU legislations to be adapted in order to further regulate the extended usage of the identity information, including fingerprints that would have been uploaded into the shared BMS. At the time this study was performed, DG HOME and eu-LISA were still studying the impacts, technical feasibility and possible scenarios for the establishment of a shared BMS. Nevertheless, this study drew the preliminary conclusion that it is technically feasible to use a shared BMS in the envisaged centralised ECRIS TCN solution. At this point in time, it can be reasonably assumed that the functions needed by the central ECRIS TCN system (i.e. storage of fingerprints and *one-to-many* matching) will be covered out-of-the-box by the shared BMS as these are basic features provided by all commercial AFIS products. The impacts of using the shared BMS would be that a different

[14] Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II).

[15] Proposal for a regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624, COM/2016/0731 final.

[16] Stronger and Smarter Borders in the EU: Commission proposes to establish an Entry-Exit System, European Commission press release, Brussels, 6 April 2016.

architecture would be put in place, although the key principles and characteristics of the centralised ECRIS TCN solution would remain identical. Regarding costs, even if the quantification of costs is not possible at this point in time, based on the qualitative data collected in this study, no significant savings would result from the integration of the centralised ECRIS TCN solution in a shared BMS. In the worst case it could even lead to additional costs when compared to the use of a dedicated AFIS in the central ECRIS TCN system.

In line with the investigation of enabling the use of ECRIS TCN by a broader audience, this study investigated the possibility of granting direct access to ECRIS TCN to third parties such as Eurojust and Europol. Providing such access to third parties would imply functional, operational and legal considerations. Similar to the impacts of integrating the ECRIS TCN solution with other EU systems, this access would need to be authorised and regulated through appropriate European and national legislation and would lead to an increased number of requests to be handled by ECRIS central authorities. Moreover, providing direct access to third parties to the centralised ECRIS TCN solution would also require technical and administrative changes, in particular: managing access rights; providing authorities with access tools to the system; providing additional training and monitoring the usage made by third parties. At this stage, it is not possible to provide cost estimates for the impact of providing direct access to third parties with the centralised ECRIS TCN solution. The main obstacle for estimating these cost impacts is the lack of detailed information on how many parties would benefit from direct accesses to the centralised ECRIS TCN solution and how many searches would be issued by them.

The functionalities enabled by a centralised ECRIS TCN solution could also increase the efficiency of ECRIS regarding EU nationals. In this context the study investigated the impacts of extending the ECRIS TCN solution by including the identity data of convicted EU nationals. This extension would eliminate the need to notify convictions of EU nationals to the Member State of nationality. Centralising the identity information and fingerprints of EU nationals would also mean that there would not be a difference in the treatment of the information and in the level of efficiency of ECRIS between EU nationals and TCN. Nevertheless, this extension would require changes in European and national legislation as well as drastic changes in ECRIS business processes as the Member State of nationality would no longer centralise the conviction information of its own nationals. At the technical level, adding the identity information of EU nationals to the central ECRIS TCN system leads to an increase in the volume of data that needs to be stored and processed at a central level, increasing the set up and operational costs of the central ECRIS TCN system. The incremental costs are mainly related to the upgrade of the central AFIS system component and the central alphanumeric search engine.

This study estimated that including EU nationals in the ECRIS TCN system would increase the cost of the centralised ECRIS TCN solution by approximately EUR 18,5 million for a nine-year period; accounting EUR 10 million one-off costs for the system implementation and EUR 1,4 million yearly ongoing costs for the system operation. The costs are higher for a highly available central ECRIS TCN system, increasing the costs by approximately EUR 30,8 million for a nine-year period;

accounting for EUR 15 million in one-off costs for the system implementation and EUR 2,6 million in yearly ongoing costs for the system operation.

Another extension to the centralised ECRIS TCN investigated in this study is the inclusion of *one-to-one* matching of fingerprints. The inclusion of this feature would enable CAs to perform additional verifications using the central ECRIS TCN system for cases where fingerprints are provided in the ECRIS request. This would help the Member States' CA by increasing the quality, reliability and efficiency of the identification of the TCN. Nevertheless, the benefits of this extension are limited given that the *one-to-many* matching done earlier by the requesting Member State is already expected to be accurate enough so as to minimise false-positive hits. The main technical impacts of this extension relate to the upgrade of the central AFIS system component.

Member States have also expressed that they would like the central ECRIS TCN system to enable them to access the identity records of TCN convicted by their Member State. This would allow each CA to have the possibility to browse, search, view, and retrieve their TCN identity records. The extension of the centralised ECRIS TCN solution to allow browsing, viewing, and retrieving features of identity records would facilitate the daily operational usage of the ECRIS TCN systems by the CA. As such features are usually provided out-of-the-box by the AFIS product, the technical impact of this extension would need additional analysis, development, testing and maintenance efforts to implement and operate these functions in the national and the central ECRIS TCN systems. At this stage, it is not possible to estimate the incremental costs of extending the centralised ECRIS TCN solution enabling browsing, viewing, and retrieving features. The main obstacle for estimating the incremental cost of this extension is the lack of information on how the functionalities and related business process would work in the context of the centralised ECRIS TCN solution.

Finally this study also evaluated the impacts of extending the centralised ECRIS TCN solution to include facial images as an additional biometric identifier. The scope of this study is limited to evaluating the impacts of capturing, uploading and storing facial images of convicted TCN so as to enable their retrieval and visual comparison by a human operator. The use of facial recognition software and the combination of facial recognition algorithms with fingerprint matching algorithms has not been assessed by this study. The main technical impact of extending the centralised ECRIS TCN solution to provide for these functions would be additional efforts in analysis, development, testing and maintenance, needed to implement these functions in both the national and the central ECRIS TCN systems. Even if additional hardware is necessary for storing the facial images in the central ECRIS TCN system, the cost impact of this storage would be negligible (e.g. facial images for TCN would amount to a total space of 100 GB; facial images for both EU nationals and TCN it would amount to a total space of 1 TB). This study estimated that extending the centralised ECRIS TCN solution to include facial images as an additional biometric identifier would increase the cost of the centralised ECRIS TCN solution by approximately EUR 0,5 million over a nine-year period; accounting for EUR 0,2 million in one-off costs for the system implementation and EUR 0,04 million in yearly ongoing costs for the system operation.

Table 1 below summaries the incremental cost impacts of the assessed extensions of the centralised ECRIS TCN solution.

Table 1 Summary of incremental costs for extensions of the centralised ECRIS TCN solution

Extensions of the centralised ECRIS TCN solution (*in million EUR, to three decimal places)*	Incremental one-off costs (3 years)	Incremental ongoing costs (1 year)
Highly available central ECRIS TCN system	6,567	1,439
Use of a shared Biometric Matching Service	Costs not available	Costs not available
Direct access by third parties	Costs not available	Costs not available
Including EU nationals to the central ECRIS TCN system	10,335	1,360
Including EU nationals to the highly available central ECRIS TCN system	14,990	2,632
Central ECRIS TCN system, Biometric verification – One-to-One matching	0,417	0,050
Highly available central ECRIS TCN system, Biometric verification – One-to-One matching	0,472	0,095
Central ECRIS TCN system including EU nationals, Biometric verification – One-to-One matching	0,435	0,060
Highly available ECRIS TCN system including EU nationals, Biometric verification – One-to-One matching	0,513	0,100
Browsing, viewing, and retrieving own identity records	Costs not available	Costs not available
Facial images as additional biometric identifiers	0,206	0,041

Source: WAVESTONE Data Analysis, March 2017.

Introduction

The European Criminal Record Information System (ECRIS) was established in April 2012[17] to make the exchange of information on criminal convictions among Member States[18] efficient. The purpose of ECRIS is to ensure that all previous convictions handed down in other Member States can be taken into account at the time of a new conviction, or for other purposes, as defined by national law.

ECRIS is a decentralised system of electronic exchange of criminal record information. To date, 28 Member States are exchanging information using this system. The system works effectively for EU nationals given that the nationality of an EU national is considered to be the 'reference' Member State nationality. Regarding Third Country Nationals and Stateless persons (TCN)[19], Member States do not know which Member State to contact with requests for criminal record information, thus resulting in either blanket requests or in no exchanges of information.

The European Commission proposed in January 2016[20] to facilitate the exchange of criminal records of TCN in the EU by upgrading ECRIS. This is a key action of the European Agenda on Security[21], which aims to improve the cooperation between national authorities in the fight against terrorism and other forms of serious cross-border crime.

Věra Jourová, Commissioner for Justice, Consumers and Gender Equality said: 'The Paris attacks in November confirmed the urgent need for more robust and seamless judicial cooperation throughout the EU. ECRIS is an important tool against cross-border crime, as it enables Member States to exchange information on previous convictions anywhere in the EU. Today we propose to upgrade this tool to ensure easier access to the convictions of non-EU citizens. Judges, prosecutors or the police will be better equipped for EU wide cooperation that will guarantee the security of all citizens throughout the EU. By including fingerprints of non-EU citizens we will have a strong tool to tackle the use of false identities.'[20]

Against this background, on 19 January 2016, the European Commission adopted a proposal[22] for a Directive amending Council Framework Decision 2009/315/JHA[18], regarding ECRIS and TCN, and replacing Council Decision 2009/316/JHA[17]. The proposal envisages the establishment of a mechanism where Member States could easily identify in which Member State(s) TCN have already been convicted

[17] 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.

[18] 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.

[19] TCN is any person who is not a citizen of the European Union within the meaning of Art. 20(1) of TFEU and who is not a person enjoying the Union right to free movement, as defined in Art. 2(5) of the Schengen Borders Code. In this context the term TCN comprises also stateless persons.

[20] European Commission - Press release, Commission proposes to strengthen the exchange of criminal records on non-EU citizens, Strasbourg, 19 January 2016.

[21] Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions, The European Agenda on Security, COM(2015) 185 final, Strasbourg, 28.4.2015.

[22] Proposal for a Directive of The European Parliament and of The Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, 19 January, Brussels.

so that the criminal record information request can be addressed to the correct Member State. This mechanism is hereafter called the ECRIS TCN solution. Furthermore, the proposal foresees the inclusion of fingerprints for the purpose of ECRIS TCN exchanges.

In order to support the European Commission on the legislative process for the establishment of the ECRIS TCN solution, feasibility studies and cost assessments were conducted in 2015[23] and 2016[24]. Among various options to implement the ECRIS TCN solution, the studies indicated that a centralised system storing alphanumeric and fingerprint identity data would be the favourite option for the implementation of the ECRIS TCN solution.

Today, the European Commission is having a second look into the technical details which should be taken into account in the ECRIS TCN legal text, inspired by the European Commission's Communication entitled 'Stronger and Smarter Information Systems for Borders and Security[25]'. Therefore, the European Commission Directorate-General for Justice and Consumers (DG JUST) mandated WAVESTONE to further assess the technical feasibility and cost impacts of implementing a centralised ECRIS TCN solution. The study also analyses:

- The interoperability, future-proofing[26], and cost impacts of the foreseen centralised ECRIS TCN solution with regard to:
    - Integration with other large-scale EU systems (including the possible need for a highly available central ECRIS TCN system);
    - Possible use of a shared Biometric Matching Service (BMS); and
    - Direct access by EU agencies;
- The impacts of a possible scope extension to the centralised ECRIS TCN solution in terms of technical optimisation, additional functionalities and future user needs. These include:
    - Inclusion of EU nationals in the central ECRIS TCN system;
    - One-to-one matching using fingerprints;
    - Browsing, viewing, retrieving by the Member State authorities of the identity records supplied by them; and
    - Use of facial images as additional biometric identifiers.

The structure of this study is as follows:

- Section 1 sets the context and background of the study;
- Section 2 describes the methodology used for assessing ICT[27] impacts;
- Section 3 describes the assessed centralised ECRIS TCN solution;

[23] Information Communication Technology (ICT) Final Report, Assessment of ICT impacts of the legislative proposal for ECRIS TCN system regarding the exchange of convictions for third country nationals and stateless people (TCN), Kurt Salmon, Brussels, 4 December 2015.

[24] Final Report, Feasibility study on the inclusion of pseudonymised fingerprints in ECRIS TCN exchanges, Kurt Salmon, Intrasoft, GLSI, Brussels, 30 June 2016.

[25] Communication from The Commission to The European Parliament and The Council, Stronger and Smarter Information Systems for Borders and Security, COM/2016/0205 final.

[26] In the context of this study, 'future-proofing' is a process of designing a software/computer system, in a way that it can still be used in the future, even when technology changes.

[27] In the context of this study, ICT stands for Information and Communications Technology.

- Section 4 presents the estimated costs for establishing a centralised ECRIS TCN solution;
- Section 5 describes the interoperability and future-proofing aspects of the central ECRIS TCN system including the cost impact of their implementation;
- Section 6 describes the options and extensions of the central ECRIS TCN system, including the cost impact of their implementation; and
- Section 7 presents the conclusions of the study.
- Annexes present additional detailed information to the study.

1 Context and background

This section presents the context and background underpinning this study, by firstly detailing the purpose, goals, main principles and challenges faced by ECRIS. Secondly, this section presents the size of the problem being tackled by the ECRIS TCN solution concerning convicted TCN in the European Union. And finally, this section provides an overview of the activities carried out up to now and the recent developments which led to the assessment of the impacts of implementing a centralised ECRIS TCN solution through this study.

1.1 European Criminal Records Information System (ECRIS)

In order to guarantee the four freedoms, free movement of goods, persons, services and capital[28], the European Union needs to ensure its citizens live in an area without internal frontiers[21], where justice and security prevail. Therefore, Member States should strengthen their collaboration and find better means to improve the cross-border exchange of criminal records information. A step forward was the establishment of the European Criminal Records Information System in 2012.

ECRIS was created with the purpose of improving the exchange of information on criminal records among Member States. In its substance, ECRIS is a decentralised system constituting an electronic interconnection between national criminal records authorities. The main purpose of ECRIS is to ensure that information on past convictions (i.e. criminal records) is exchanged among Member States in a uniform and speedy way. The system provides judges and prosecutors with easy access to comprehensive information on the criminal history of persons concerned, no matter which Member States had convicted the person in the past. The system serves to prevent crime, by eliminating the possibility of offenders to evade their criminal past by simply moving from one Member State to another.

The exchange of information through ECRIS is performed using a standardised electronic format available in all EU languages. The standardisation (i.e. common ECRIS codes, offences and sanctions are mapped against national offences and sanctions) of all ECRIS exchanges allows for an efficient, immediate and intelligible communication among Member States. Designated central authorities (i.e. National Competent Authorities) in every Member State are the contact points for the ECRIS network, responsible for storing, collecting and providing criminal records information.

The general principles of ECRIS are the following[29]:

- ECRIS is based on a decentralised IT[30] architecture, where criminal records' data is stored solely in national databases of Member States and are exchanged electronically between the Central Authorities of Member States, upon request.

[28] Consolidated version of the Treaty on European Union, Official Journal of the European Union, Brussels, 26.10.2012.
[29] 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.
[30] In the context of this study, IT stands for Information Technology, defined as "the common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services." (Gartner IT Glossary)).

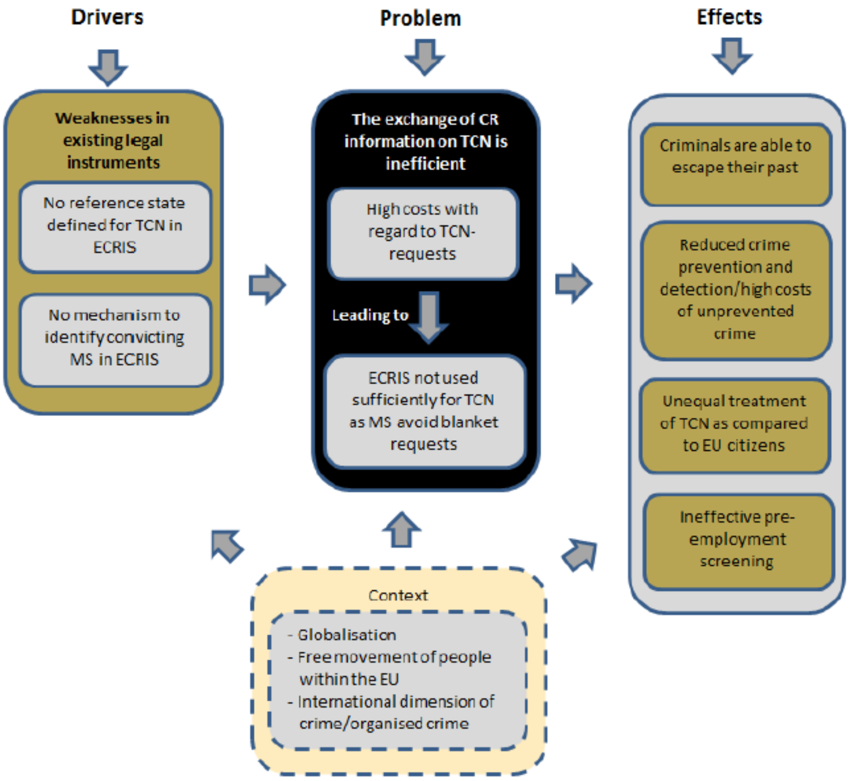
- The Member State of nationality of a person becomes the central repository for all convictions handed down against that person. The Member State of nationality is obliged to store and update all the information received, as well as to retransmit all information when requested. As a result, each Member State should be in a position to provide exhaustive and up-to-date information in relation to its nationals' criminal records, upon request from others Member States and regardless of where those convictions were handed down.
- A Member State convicting a citizen from another Member States is obliged to immediately send information, including updates, on the conviction to the Member State(s) of the offender's nationality.
- The transmission of information on convictions is made electronically, through a standardised European format, using two reference tables for offences and penalties' categories. These tables facilitate automatic translation and enhance mutual understanding of the information transmitted. When transmitting information on a conviction, a Member State has to indicate appropriate codes for the category of an offence and the penalty or sanction, which is automatically translated into the language of the recipient, enabling the addressed Member State to react immediately upon receipt of the information.

Up to now, ECRIS proves to work efficiently with regard to EU nationals, however, ECRIS faces challenges finding the Member State(s) holding past convictions of Third Country Nationals and Stateless persons (TCN). The following section elaborates on this point.

1.2 ECRIS challenges regarding the exchange of previous convictions of TCN

Currently the operation of ECRIS regarding exchange of information on previous convictions of TCN among Member States for judicial and other purposes is inefficient. According to the general principles of ECRIS, the Member State of nationality of a person becomes the central repository of all convictions handed down against that person, which makes the identification of the Member State holding the past criminal records of convicted EU national easier. However, as TCN have no Member State nationality, a Member State prosecuting a TCN does not know which Member State(s) might have past criminal records of that person. This is explained by the fact that criminal records information of TCN is kept in the national registers of the respective convicting Member State(s). Therefore, the only possibility to obtain a full overview of the criminal history of a convicted TCN is to send a request to all Member States, even though the criminal records information regarding the convicted TCN could exist only in one or few Member States. This inefficiency leads to a significant administrative burden and often to a situation where request are not made at all. Figure 2 below sets out the ECRIS problem in the form of a problem tree.

Figure 2 ECRIS TCN problem tree


Drivers
Problem
Effects
Weaknesses in existing legal instruments
No reference state defined for TCN in ECRIS
No mechanism to identify convicting MS in ECRIS
The exchange of CR information on TCN is inefficient
High costs with regard to TCN-requests
Leading to
ECRIS not used sufficiently for TCN as MS avoid blanket requests
Criminals are able to escape their past
Reduced crime prevention and detection/high costs of unprevented crime
Unequal treatment of TCN as compared to EU citizens
Ineffective pre-employment screening
Context
- Globalisation
- Free movement of people within the EU
- International dimension of crime/organised crime

Source: ECRIS Impact Assessment[31].

The second major challenge that ECRIS faces is the identification of the specific convicted person. A reliable system for the exchange of information on convictions requires a sufficient degree of certainty regarding the data identifying a specific person. Establishing the identity of a TCN can be challenging because of the use of different alphabets, languages, common surnames or because reliable identity documents are not available. Additionally, the use of aliases and false identities is also common among those seeking to escape identification.

Identity criteria used by Member States in their criminal record systems tend to vary considerably. Some Member States rely on names (of the person concerned, the father's name, the mother's name, or both), date and place of birth, nationality, country of birth and sex to confirm a person's identity. Others require a registration number. Yet other countries have organised identification of persons based on fingerprints. Despite the differences, Member States have reached an agreement on the compulsory and optional information to be exchanged through ECRIS regarding requests on convicted persons. Regarding fingerprints, ECRIS provides for the exchange of fingerprints on a voluntary basis in addition to the exchange of alphanumeric identity information. At present, the Member State of nationality may store fingerprints (according to national law), which have been transmitted as part of a conviction notification. Member States' central authorities are obliged to transmit fingerprints which have been taken from convicted persons to the Member State of nationality, where fingerprints are available to the

[31] Impact Assessment accompanying the proposal for a Directive of the European Parliament and of the Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, dated 2016.

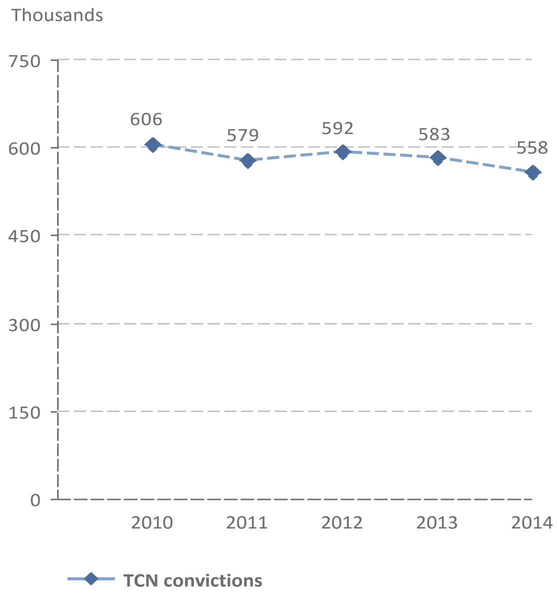
central authority. Against this background and according to the Commission's proposal[32], the inclusion of fingerprints as biometric identifiers for the purposes of ECRIS exchanges should be treated as a priority.

1.3 TCN convictions – the size of the problem

As elaborated in the section 1.2, ECRIS does not cope successfully with the exchanges of TCN criminal records. According to Eurostat information[33], TCN residing legally in the EU on 1 January 2015 accounted for around 4% of the total EU population, which brings the total number of TCN legally residing in the EU to around 20 million persons.

Surveys conducted by the European Commission in 2015 under the work supporting the ECRIS TCN Impact Assessment[34] have looked at the volume of convictions of TCN in the EU. The outcome of the surveys is illustrated in Figure 3 below. The graph represents the number of convictions of TCN in the EU over a five-year period, based on statistics collected from 19 Member States. As not all Member States provided information, the total number of TCN convictions is expected to be higher.

Figure 3 Number of TCN convictions per year in the EU (19 Member States)



Source: ECRIS TCN Impact Assessment 2016[34]

Furthermore, according to a number of studies carried out, including the 2010 Unisys[35] and 2015 Kurt Salmon[36] studies, Figure 4 below provides an overview of the most recent estimated volume of TCN convictions distributed across Member States.

[32] Proposal for a Directive of The European Parliament and of The Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, 19 January, Brussels.

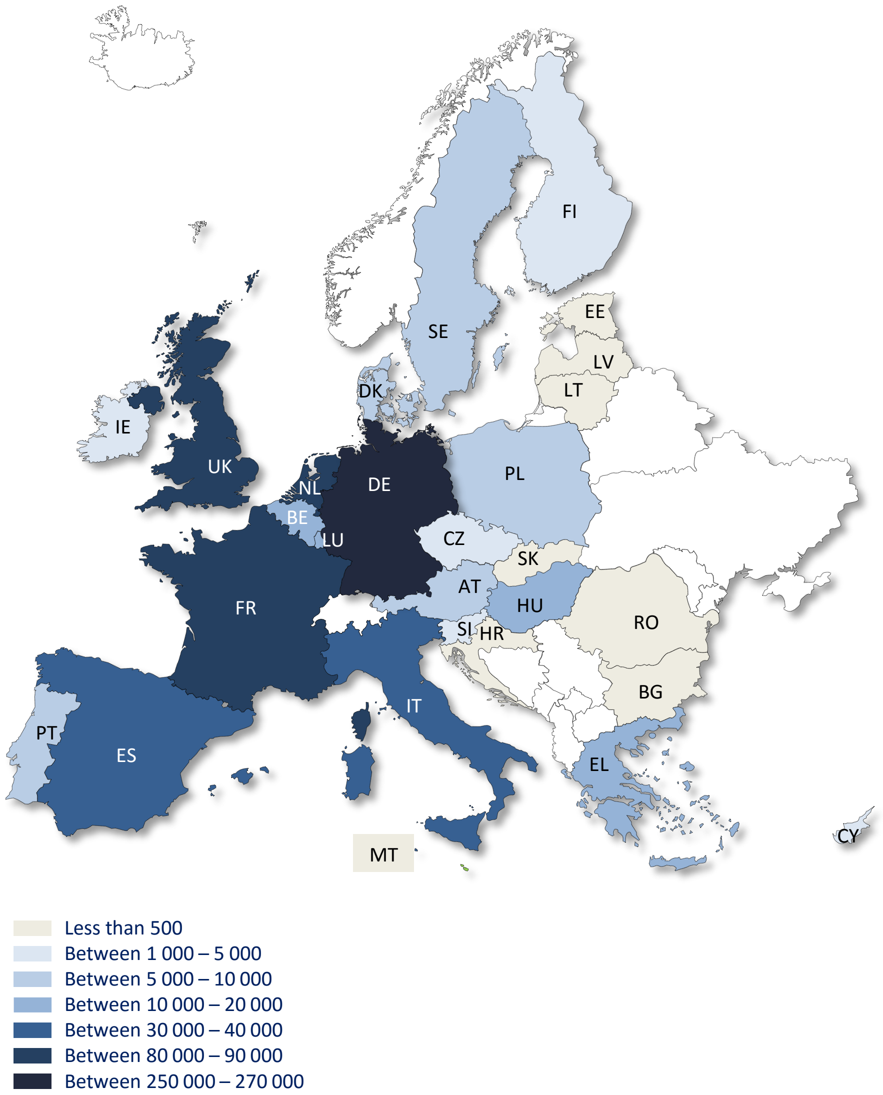
[33] Migration and migrant population statistics, Eurostat, Data extracted in May 2016.

[34] Impact Assessment accompanying the proposal for a Directive of the European Parliament and of the Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, dated 2016.

[35] Feasibility Study: Establishment of a European Index of Convicted Third Country Nationals, Unisys, 2010.

[36] Information Communication Technology (ICT) Final Report, Assessment of ICT impacts of the legislative proposal for ECRIS TCN system regarding the exchange of convictions for third country nationals and stateless people (TCN), Kurt Salmon, Brussels, 4 December 2015.

Figure 4 Number of TCN convictions in the EU in 2014



Source: ICT Final Report, Kurt Salmon, Brussels 2015[36]

Based on all analysed data regarding volumes of convictions of TCN within the EU, it can be concluded that in the period 2010 to 2014 there were on average 700 000 convictions of TCN recorded per year. Furthermore, according to ECRIS internal statistics, in 2014, only 23 000 requests were made concerning convicted TCN. This fact implies that approximately 95% of the total number of TCN convictions for 2014 were handed down without the use of ECRIS regarding possible previous convictions of individuals in another Member State(s). This means that for increasing the collaboration across Member States with regard to the exchange of past criminal records of convicted TCN, the ECRIS system should be improved, which will consequently help combating organised crime and terrorism in EU.

The number of convictions related to TCN are estimates based on data provided by Member States as well as on data extrapolation techniques. In this study, these estimates are used exclusively for cost assessment purposes in order to size the future system that needs to be developed.

1.4 The centralised ECRIS TCN solution – the way ahead

In 2015, the European Agenda on Security[37] set out the need for easy access to criminal convictions of TCN as one of its priorities. Following this direction, the Commission has worked towards investigating possible technical solutions to improve ECRIS by tackling the main challenges regarding the exchange of TCN criminal records. Specifically, the Commission mandated two studies assessing the technical feasibility and associated costs of technical options. The first study[38] focused on the comparison between two scenarios for the implementation of an ECRIS TCN mechanism that could be summarised as follows:

- A decentralised mechanism where an index containing alphanumeric identity convicted TCN would be exchanged among all Member States; and
- A centralised mechanism where an index containing alphanumeric identity of convicted TCN would be stored at a central level in a system operated by the European Union, possibly by the European Agency for the Operational Management of large scale Information Technology Systems in the Area of Freedom, Security and Justice (eu-LISA).

The index would be searched by all Member States to identify other Member States holding criminal records information on a particular TCN. The search would produce a 'hit' or 'no-hit' reply. A 'hit' would provide information on i) whether the person concerned has already been convicted in another Member State and ii) which Member State(s) to address to receive information on this conviction. After a 'hit' (or several hits), the requesting Member State can contact directly the identified Member States(s) through the established ECRIS network.

It is well accepted that ECRIS should be a system providing a sufficient degree of certainty regarding the data identifying a specific person, in order to be considered as a reliable system for exchanging information on convictions. Following up on the first study and based on several meetings with ECRIS experts from Member States, the Commission concluded that the use of fingerprints in an ECRIS TCN solution is essential. This conclusion was supported by the fact that establishing the identity of TCN using solely alphanumeric data is known to be problematic because of the use of different alphabets, languages, common surnames or because reliable identity documents are frequently not available. Therefore, a second study[39] assessed the feasibility and associated costs for the inclusion of fingerprints in the ECRIS exchanges.

Overall, the second study[39] concluded that a centralised mechanism for implementing the ECRIS TCN solution including alphanumeric identify data and fingerprints, is overall less complex and less costly to implement compared to a decentralised mechanism. Furthermore, an important consideration favouring a centralised mechanism relates to the benefits arising from proven technologies and successful

[37] Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions, The European Agenda on Security, COM(2015) 185 final, Strasbourg, 28.4.2015.

[38] Information Communication Technology (ICT) Final Report, Assessment of ICT impacts of the legislative proposal for ECRIS TCN system regarding the exchange of convictions for third country nationals and stateless people (TCN), Kurt Salmon, Brussels, 4 December 2015.

[39] Final Report, Feasibility study on the inclusion of pseudonymised fingerprints in ECRIS TCN exchanges, Kurt Salmon, Intrasoft, GLSI, Brussels, 30 June 2016.

implementations of already existing and comparable fully automated centralised systems (e.g. EURODAC[40] and VIS[41]).

Following the June 2016 Justice and Home Affairs Council, where a large majority of Member States had indicated support for implementing a centralised solution for ECRIS TCN, and inspired by the Commission's communication 'Stronger and Smarter Information Systems for Borders and Security'[42], the Commission has had another look in detail at the technical, legal and policy issues which follow from this preference. This second look called for a study on the technical feasibility and cost impact to implement a centralised ECRIS TCN solution as well as to analyse the interoperability, future-proofing, and possible extensions of the foreseen system.

The following section describes the overall methodology used to conduct this study.

[40] Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of the Dublin Convention, 11 December 2000.

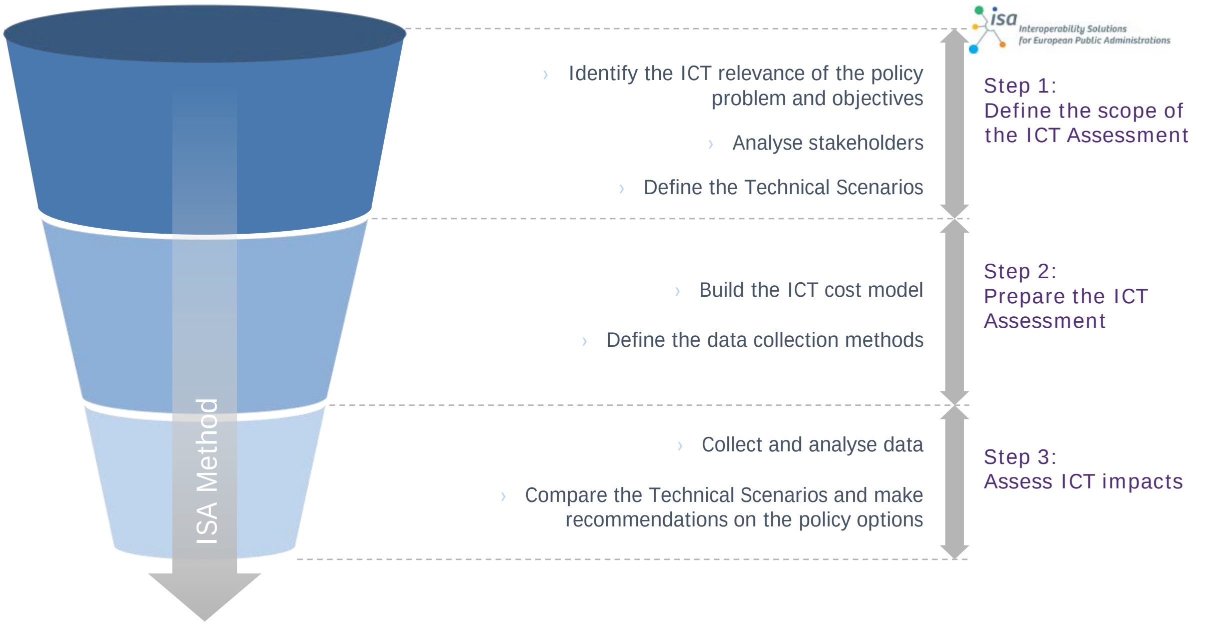
[41] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), 9 July 2008.

[42] Communication from the Commission to the European Parliament and the Council, Stronger and Smarter Information Systems for Borders and Security, COM(2016) 205 final, Brussels, 6.4.2016.

2 Methodology

The *Feasibility study and cost assessment of the establishment of a centralised ECRIS TCN solution* follows a set of logical steps as proposed in the ISA Method[43]. These steps are designed in a way that prepares evidence for political decision-makers on the advantages and disadvantages of possible policy options by assessing their potential impacts. The ISA Method, presented in Figure 5 below, was developed by the ISA Programme[44] and is referred in the Better Regulation Guidelines from the Commission[45]. It comprises three steps, namely: Step I: Define the scope of the ICT Assessment; Step II: Prepare the ICT Assessment; Step III: Assess the ICT impacts.

Figure 5 ISA Method – overall approach


isa Interoperability Solutions for European Public Administrations
ISA Method
› Identify the ICT relevance of the policy problem and objectives
› Analyse stakeholders
› Define the Technical Scenarios
Step 1: Define the scope of the ICT Assessment
› Build the ICT cost model
› Define the data collection methods
Step 2: Prepare the ICT Assessment
› Collect and analyse data
› Compare the Technical Scenarios and make recommendations on the policy options
Step 3: Assess ICT impacts

The ISA Method aims to enable public administrations, at both EU and national levels, to better estimate the ICT impacts of proposed EU legislation, ideally prior to their adoption by the European Parliament (EP) and the Council (i.e. ordinary legislative procedure), meaning both during the legislative proposals' preparation and approval phases, but also later, once the legislation has been adopted.

In the scope of the current study, the ICT Impact Assessment is focused on two main criteria: cost efficiency, the incremental costs (i.e. non-business as usual) to the target group of complying with the regulation other than fees and administrative costs) and technical feasibility of the proposed technical solutions. The detailed methodology followed in this study is presented in Annex I.

[43] The ISA Method for Assessing ICT Implications of EU Legislations is applied to the assessment of cost impacts, 2015.
[44] The ISA Programme, run by DG DIGIT, was designed to support and facilitate efficient and effective cross-border and cross-sector interoperability. The programme takes integrated approach to enhancing interoperability through more than 40 actions with a goal to ease cross-border and cross-sector electronic collaboration between public administrations. In November 2015, the follow-up programme to ISA, ISA^2, was officially adopted by the European Parliament and the Council of the European Union.
[45] Better Regulation Guidelines [COM (2015)205 final] European Commission, 19.05.2015.

3 Description of the centralised ECRIS TCN solution

This section describes the high-level architecture, key principles and processes of the envisaged centralised ECRIS TCN solution. It also provides information regarding the technical assumptions, requirements and system characteristics.

3.1 Architecture and key principles

ECRIS is by nature a decentralised system. Currently each Member State operates its own installation of the ECRIS system. The exchanges of information are done on a bilateral basis, directly between Member States, without relying on a centralised component. These message exchanges take place on the secured TESTA-ng[46] communication network.

Bilateral exchanges are only possible if the requesting Member State knows to which other Member State it should send the request for information on criminal records. For EU nationals, the legal framework of ECRIS has established that the Member State of nationality serves as point of reference. The Member State of nationality thus stores all information on convictions handed down against its nationals, including convictions handed down in other EU Member States. The current system works well and is efficient for EU nationals. It should be noted that good results are obtained already based largely only on alphanumeric identity information. Fingerprints are supported but are not used widely throughout the EU; only a few Member States currently use them for EU nationals.

For third country nationals (TCN), the first difficulty is to find out which Member State(s) possibly hold(s) information on past convictions so as to avoid systematically querying all EU Member States. The second difficulty lies in the proper identification of the TCN.

The conclusions of the feasibility study on the inclusion of pseudonymised[47] fingerprints in ECRIS TCN exchanges conducted in 2016[48], as well as the subsequent discussions with Member States, led the Commission to focus on a centralised solution for ECRIS TCN, relying on the systematic usage of fingerprints as a means to cope with these two issues.

However, the centralised ECRIS TCN solution must be seen as a complement to the current ECRIS system, which remains decentralised. The centralised ECRIS TCN solution only serves the purpose of holding the identity records (alphanumeric identity information and fingerprints) of all TCN convicted in the EU in view of determining which Member State(s) need to be queried in case information on past

[46] TESTA-ng (Trans European Services for Telematics between Administrations) provides e-communication services for data exchanges required for the implementation of any European policies. It is the European Community's own private network enabling data exchange between Member States, EU Institutions and EU Agencies. The TESTA-ng network is part of ISA^2 Action Strengthening the EU's telecommunications backbone, Data communication network service (TESTA/sTESTA/TESTA-ng).

[47] 'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (EU Data Protection Directive: Article 3 (5) of Directive (EU) 2016/680).

[48] Final Report, Feasibility study on the inclusion of pseudonymised fingerprints in ECRIS TCN exchanges, Kurt Salmon, Intrasoft, GLSI, Brussels, 30 June 2016.

convictions is requested for a TCN. The accurate identification of the TCN normally takes place at a later stage, within the Member State(s) that have been queried by the ECRIS system for information on past convictions, and for finding the corresponding criminal records (if any).

For the purpose of this study, at national level several groups of stakeholders are considered:

- The ECRIS Central Authority (CA) is responsible for all ECRIS exchanges. For the sake of simplicity, it is considered that the CA also operates the national criminal records register. The CA operates the following systems:
  - The national criminal records register that stores the information on convictions, which includes (i) convictions of its own nationals handed down in any Member State and (ii) convictions of TCN handed down in the Member State.
  - The ECRIS system used for exchanging information on criminal records with other Member States.
  - The new national ECRIS TCN system providing features for storing, processing and handling TCN alphanumeric identity information and fingerprints.
- Judicial authorities: all authorities within the Member State handing down convictions (e.g. courts, prosecutors, etc.). These authorities provide the information on convictions to the CA.
- Executive organisations: entities involved in the enrolment and transmission of fingerprints of TCN to the CA.

This study assesses a centralised solution for ECRIS TCN composed of two new, distinct software systems:

(1) The central ECRIS TCN system, set-up and operated by eu-LISA:

- This system stores alphanumeric identity information and fingerprints of all TCN convicted in all EU Member States.
- The identity records of convicted TCN are used in the central ECRIS TCN system <u>for the sole purpose of enabling a centralised 'hit/no hit' search</u>.
- A Member State seeking to find the past criminal history of a given TCN performs a 'hit/no hit' search using the central ECRIS TCN system for identifying which other Member State(s) can be queried for information about these past convictions. Basically, the central ECRIS TCN system is answering the question '*Which other Member State(s) possibly hold(s) past information on convictions for this specific TCN?*'

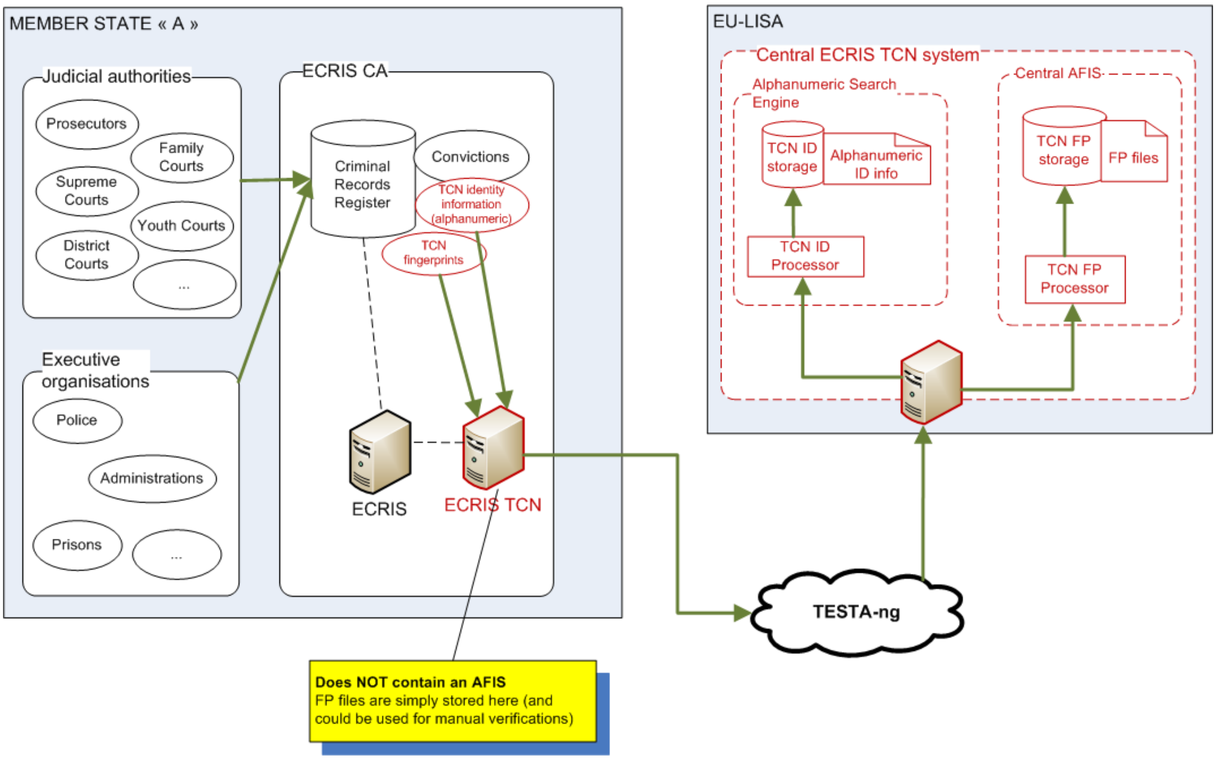
(2) The national ECRIS TCN system, set-up and operated by each Member State's CA:

- This system integrates with the national criminal records register and with the central ECRIS TCN system for uploading identity records of TCN that were convicted at national level.
- In case the CA needs to issue a request for information on past convictions relating to a TCN, this application can automatically query the central ECRIS TCN system by triggering a 'hit/no hit'

search. It integrates at national level with the existing ECRIS system for automatically preparing ECRIS requests targeting the Member State(s) for which the search returned a hit.

Figure 6 below shows the overall architecture of the centralised ECRIS TCN solution.

Figure 6 Centralised ECRIS TCN solution: Architecture



Does NOT contain an AFIS
FP files are simply stored here (and could be used for manual verifications)

The overall solution relies on the central ECRIS TCN system holding both alphanumeric identity information and fingerprints. The proposed architecture has the following key characteristics:

- The central ECRIS TCN system is put in place, operated by eu-LISA.
- Fingerprints and alphanumeric identity data of TCN convicted throughout the EU are stored in the central ECRIS TCN system for the sole purpose of enabling a centralised 'hit/no hit' search.
- A Member State seeking to find the past criminal history of a particular TCN performs first a 'hit/no hit' search in the central ECRIS TCN system, through its national ECRIS TCN system, for identifying which other Member State(s) can be queried for information about these past convictions.

The Member States do not share directly among them any identity information regarding convicted TCN. The identity information is centralised in an EU-wide system dedicated for the purpose of ECRIS TCN and managed by eu-LISA.

When a TCN is convicted in a given Member State, the identity information and fingerprints of the TCN are entered by the CA into the national ECRIS TCN system. The national ECRIS TCN system transmits the alphanumeric identity information and the associated fingerprints to the central ECRIS TCN system for storage.

When a Member State needs to search for information on past convictions of a given TCN, the CA of the requesting Member State uses its national ECRIS TCN system to find whether this TCN has previous convictions within the EU. The national ECRIS TCN system automatically contacts the central ECRIS TCN system in order to perform a 'hit/no hit' search using both alphanumeric identity information and fingerprints, to find which other Member States possibly have information on past convictions. The CA then prepares an ECRIS request and sends it to the Member State(s) that were identified as a result of the 'hit/no hit' search.

3.2 Processes

This section describes in detail how the various ECRIS TCN business processes work using the architecture presented in section 3.1. This allows the reader to have a better understanding of the complexity and functioning of the centralised ECRIS TCN solution and its subsystems. It also provides an understanding of the main cost items that are assessed in this study. It should be noted that the processes occurring within Member States are out of the scope of this study; the following process descriptions focus on the usage of the national and central systems of the centralised ECRIS TCN solution.

3.2.1 Registration of TCN identity information into the national ECRIS TCN system

The process starts when a national court has convicted a TCN:

(1) The CA receives from the convicting authority the information on the conviction of the TCN. This set of information contains alphanumeric identity information of the TCN, information on the offences committed and sanctions that were pronounced.

(2) The CA collects or receives from an executive organisation (for example from a police office) the fingerprints of the convicted TCN, in the form of a NIST file[49] matching the technical specifications and minimum quality criteria defined for the ECRIS TCN solution.

(3) The CA first stores the conviction information and identity information of the TCN in the national criminal records register.

(4) Then the CA enters the identity information and NIST file containing the fingerprint images into the national ECRIS TCN system. In addition, the CA should also provide a unique technical reference to the national ECRIS TCN system (for example a unique identifier for the fingerprint records). This reference is known in the national criminal records register and serves in the later processes for finding back the corresponding conviction data.

Please note that this step can be done automatically by the national criminal records register if it is technically integrated with the national ECRIS TCN system.

[49] NIST is a standardised data format for interchange of fingerprint, facial and other biometric information.

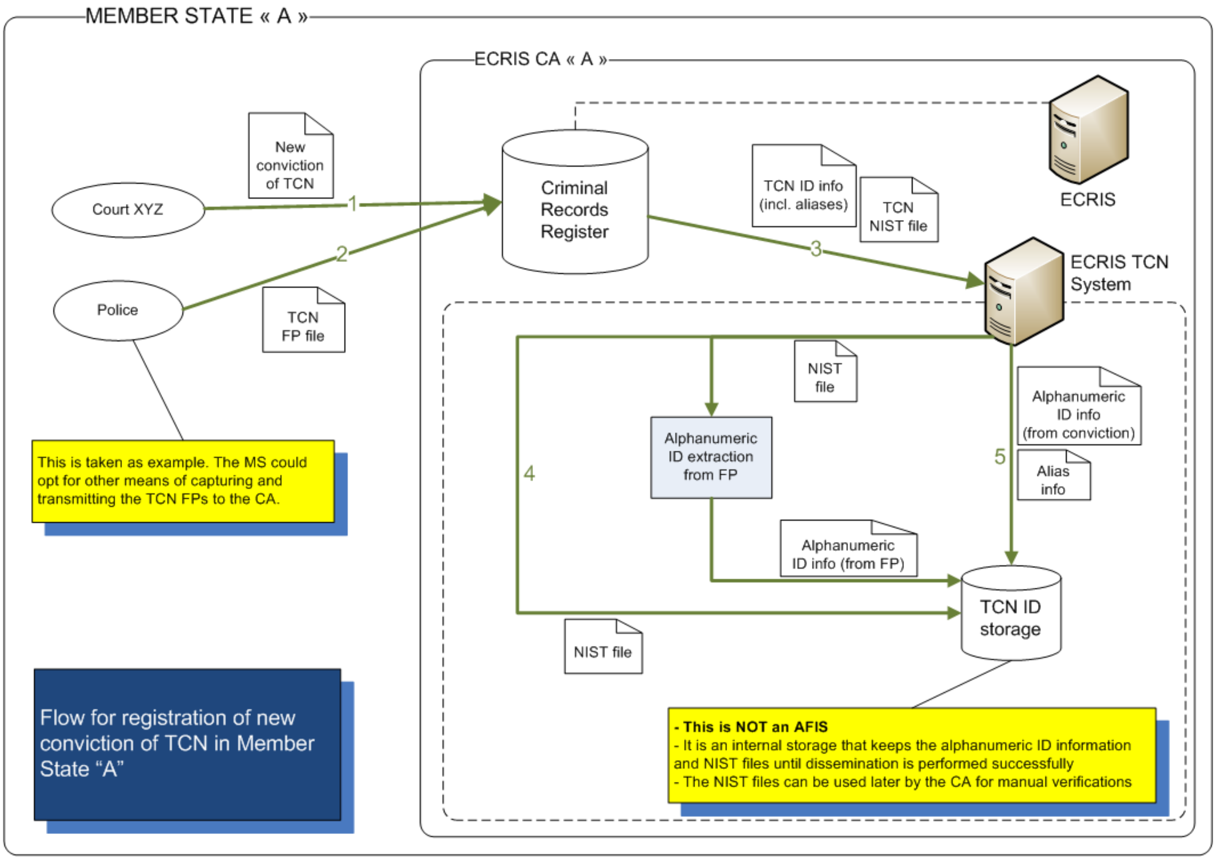
(5) The national ECRIS TCN system extracts the alphanumeric identity information, including aliases and possibly alphanumeric identity information contained in the NIST file. Then it stores the alphanumeric identity information and the NIST file (including also the unique technical reference).

It should be noted that national ECRIS TCN system is not an Automated Fingerprint Identification System (AFIS). It is assumed to contain a simple internal storage, such as a database and/or file system.

The alphanumeric content held in the NIST file next to the fingerprint images can be different from the alphanumeric identity information supplied with the conviction. This depends on when and how the fingerprints were collected at national level. It could be the case that the fingerprints were captured by an executive administration several months or years, before the conviction is handed down against the TCN, and thus a long time before the alphanumeric identity information is captured together with the information on offences and sanctions. This may lead to differences that must be taken into account in the ECRIS TCN solution. This study assumes that the alphanumeric information contained in the NIST file should be extracted and should be considered as an additional alias (in case that it is different from the primary alphanumeric identity information).

Figure 7 below shows the process of registering TCN identity information into the national ECRIS TCN system.

Figure 7 Registration of TCN identity information into the national ECRIS TCN system



This is taken as example. The MS could opt for other means of capturing and transmitting the TCN FPs to the CA.

Flow for registration of new conviction of TCN in Member State "A"

- **This is NOT an AFIS**
- It is an internal storage that keeps the alphanumeric ID information and NIST files until dissemination is performed successfully
- The NIST files can be used later by the CA for manual verifications

3.2.2 Upload of TCN identity information into the central ECRIS TCN system

The process is triggered by the national ECRIS TCN system after new TCN information has been entered at national level. It can take the form of a periodic job running regularly or to be triggered systematically whenever new data is registered in the national ECRIS TCN system.

(1) Member State 'A' has previously convicted a TCN and entered the identity information in its national ECRIS TCN system. The national ECRIS TCN system now uploads the TCN's alphanumeric identity information and fingerprints to the central ECRIS TCN system. The national ECRIS TCN system includes the unique technical reference and transmits it to the central ECRIS TCN system along with the identity information.

(2) The data is transmitted over the secured TESTA-ng communication network. It is assumed that encryption is performed at network-level (for example using HTTPS and security certificates).

(3) The central ECRIS TCN system performs 2 tasks:

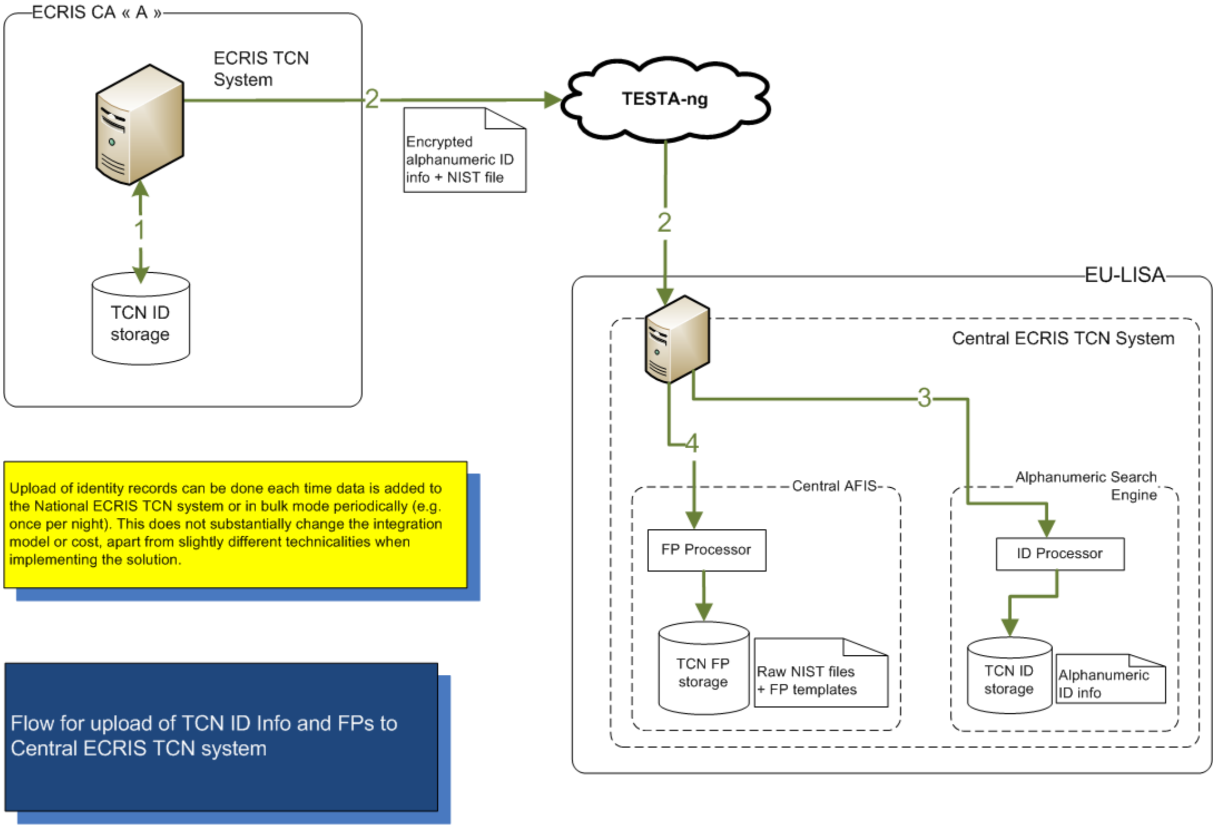
a. It provides the alphanumeric identity information internally to its alphanumeric search engine. Its internal ID processor performs the necessary transformations and indexation of the alphanumeric data for optimising the searches, especially the fuzzy searching[50] required later. The alphanumeric identity information is stored internally.

b. It provides the NIST file as input to its internal AFIS. The fingerprint processor of the AFIS subcomponent extracts the minutiae information from the fingerprint images contained in the NIST file and generates fingerprint templates (i.e. a binary representation of the fingerprint minutiae) that are used for *one-to-many matching* required later. The AFIS stores internally the fingerprint templates, the NIST file containing the raw fingerprint images and the unique technical reference provided by the uploading Member State.

Figure 8 below shows the process of uploading TCN identity information into the central ECRIS TCN system.

[50] For the purpose of this study, the term *fuzzy searching* (fuzzy logic) refers to a computer algorithm that enables searches of alphanumeric data that match a pattern approximately (rather than exactly). The results of *fuzzy*searching include by definition records that exactly match the search criteria but also records that are not strictly equal but considered similar by the system by not excluding exact matches.

Figure 8 Upload of TCN identity information into the central ECRIS TCN system



Upload of identity records can be done each time data is added to the National ECRIS TCN system or in bulk mode periodically (e.g. once per night). This does not substantially change the integration model or cost, apart from slightly different technicalities when implementing the solution.

At this stage, the details of when and how the upload of data to the central ECRIS TCN system is done from a technical point of view is unknown. For the purpose of this study it is assumed that this will technically rely on the usage of a form of remote, secured services (e.g. web services), which could be synchronous or asynchronous. Uploading could also be done each time data is added or in bulk mode periodically (e.g. once per night). Such implementation details however do not significantly affect the estimated costs.

3.2.3 Central 'hit/no hit' search for identifying Member States holding conviction data

The central 'hit/no hit' search process is triggered individually by a Member State when, at national level, a competent authority contacts its national ECRIS Central Authority (CA) to request information on past convictions of a given TCN. Typical competent authorities are judicial authorities (courts, prosecutors, etc.) and national administrations (for issuing specific types of permits, for purposes of employment, etc.).

The 'hit/no hit' search mechanism aims at identifying the Member State(s) holding information on past convictions of a given TCN subject.

(1) The requesting competent authority provides to the CA the identity of the TCN as well as the fingerprints, where available.

(2) The CA then enters all TCN information into the national ECRIS TCN system to trigger a 'hit/no hit' search.

(3) The ECRIS TCN system of the requesting CA automatically forwards the whole set of information (alphanumeric identity information and fingerprints) to the central ECRIS TCN system via the secured TESTA-ng network.

(4) The central ECRIS TCN system performs internally the following tasks:

a. Using the NIST file received as input, it triggers a **one-to-many** matching using its internal AFIS. The AFIS responds internally to the central ECRIS TCN system with a list of hits, including the unique technical reference provided by the convicting Member State for the fingerprints that caused the hits.

b. Using the alphanumeric identity information received as input, it triggers a search using its internal alphanumeric search engine. This also results possibly in a list of Member States with hits.

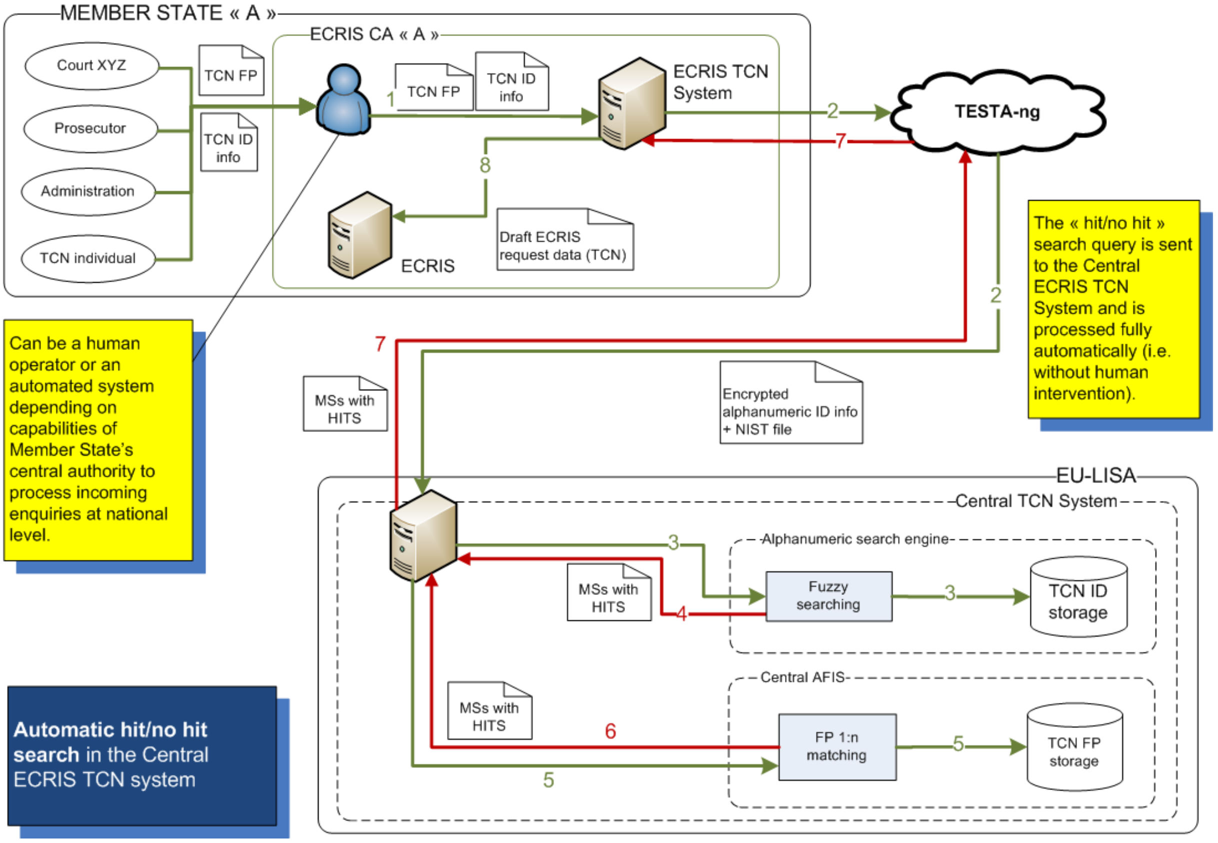
(5) The central ECRIS TCN system then consolidates both lists of Member States with hits and provides it as a response to the national ECRIS TCN system of the requesting Member State. The response may also include the alphanumeric or fingerprint information of the TCN identities that raised the hits.

(6) Upon receipt of hits, the ECRIS TCN system of the requesting Member State could then automatically generate draft ECRIS requests targeting the Member States that were identified.

It is important to note here that the central 'hit/no hit' search must be fully automated and take place without human intervention, as it is expected that a considerable number of 'hit/no hit' searches will need to be performed per day.

Figure 9 below shows the process of automated 'hit/no hit' search using the central ECRIS TCN system.

Figure 9 Automated 'hit/no hit' search using the central ECRIS TCN system



Can be a human operator or an automated system depending on capabilities of Member State's central authority to process incoming enquiries at national level.

The « hit/no hit » search query is sent to the Central ECRIS TCN System and is processed fully automatically (i.e. without human intervention).

Automatic hit/no hit search in the Central ECRIS TCN system

3.2.4 Decentralised ECRIS requests for collecting information on past convictions of TCN

This process starts after the 'hit/no hit' search has been done using the TCN identity information (alphanumeric and/or fingerprints). At this moment the national ECRIS TCN system of the requesting Member State has prepared a draft ECRIS request message targeting the Member State(s) identified in the previous step (section 3.2.3).

(1) In Member State 'A', the CA verifies and completes the ECRIS requests. When ready, the CA sends off the ECRIS request messages to the Member State(s) that were previously identified. Each ECRIS request contains the alphanumeric identification information, an attached NIST file with the fingerprint images where available and a unique technical reference associated with the fingerprints that produced the 'hit'.

(2) Each Member State which receives the ECRIS request message processes it according to the current mechanisms in ECRIS. The CA of each requested Member State looks whether information on past convictions can be found corresponding to the TCN identity information sent in the ECRIS request. This search at national level is done differently in each Member State depending on the tools and data that are available to the CA.

(3) In ECRIS, it is always the responsibility of the requested Member State to identify the person that is subject of the request, because ultimately it is also the requested CA that takes the responsibility of sending back, or not, information on past convictions found in the national criminal records register.

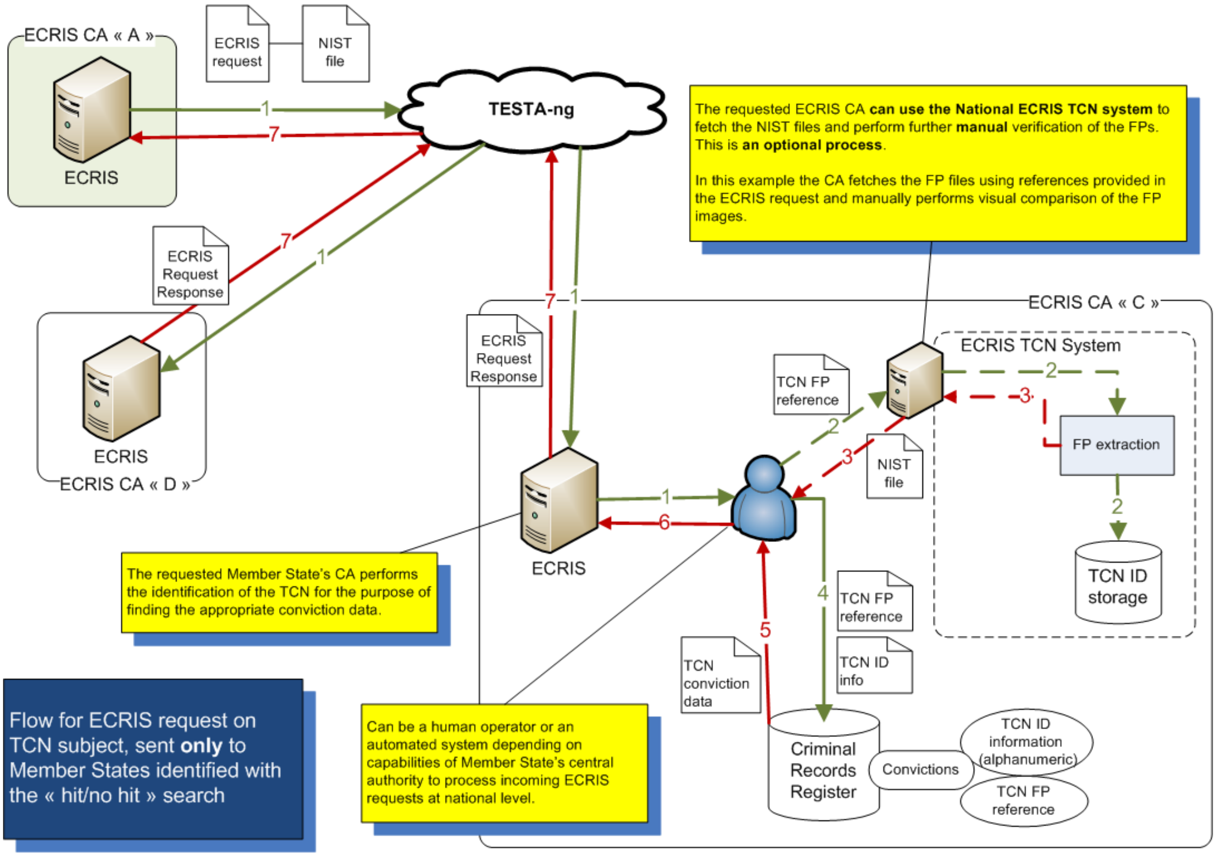
(4) The CA may use the national ECRIS TCN system for retrieving the identity records (alphanumeric and fingerprints) that provoked the 'hit' at central level and for comparing them visually with the TCN identity information provided by the requesting Member State in the ECRIS request.

(5) The CA of each requested Member State prepares an ECRIS response with the information found at national level in the criminal records register and sends it back to the requesting Member State.

(6) Finally, the ECRIS system of the requesting Member State consolidates all the responses received from the requested Member State(s).

Figure 10 below shows the process of ECRIS requests relating to a TCN sent to multiple Member States.

Figure 10 ECRIS request relating to a TCN sent to multiple Member States



The requested ECRIS CA **can use the National ECRIS TCN system** to fetch the NIST files and perform further **manual** verification of the FPs. This is **an optional process**.

In this example the CA fetches the FP files using references provided in the ECRIS request and manually performs visual comparison of the FP images.

The requested Member State's CA performs the identification of the TCN for the purpose of finding the appropriate conviction data.

Flow for ECRIS request on TCN subject, sent **only** to Member States identified with the « hit/no hit » search

Can be a human operator or an automated system depending on capabilities of Member State's central authority to process incoming ECRIS requests at national level.

NOTE: In the previous processes, at no point is the AFIS within the central ECRIS TCN system used for identifying the TCN subject. It is only used for finding a list of Member States possibly holding information on past convictions for this TCN. Actual identification takes place at a later stage during the ECRIS exchanges, at national level. In ECRIS, the Member State that is requested to provide information on criminal records bears the responsibility for performing this identification, for the sole purpose of finding the corresponding conviction data. The requesting Member State does not need to perform identification of the person for which past convictions are requested. It must also be noted that several Member States, when requested, do not even perform the identification of the person at all but rather search conviction records based on the provided set of identities. The identification of the person must be seen only as a possible means to find the corresponding conviction data. This is a major difference with the typical usage of AFIS systems in law-enforcement bodies, where the focus lies on confirming the identity of a person. In the judicial business processes, identification of the person takes place at other moments and with other means (before or when appearing in court, before or when registering conviction data in the national criminal records register, when the convicted person starts executing the sanction, etc.).

3.3 Assumptions, requirements and system characteristics

In order to estimate costs it is necessary to have a general idea of the expected features and characteristics of the systems to be designed, implemented, tested, deployed and operated.

This section provides a high-level description of the key requirements for the national ECRIS TCN system and for the central ECRIS TCN system. In addition, it also elaborates on the major changes that need to be foreseen to the existing ECRIS systems.

3.3.1 Technical assumptions and system requirements

This section describes the general technical assumptions and system requirements that are applicable to all components of the centralised ECRIS TCN solution.

- Quality of the biometric data: fingerprints are assumed to be taken in controlled conditions and are expected to be of good quality (10-print fingerprints or enough prints taken of good quality – no latent or crime-scene fingerprints). In particular, this study is based on the assumption that all the fingerprints captured, stored and transported across the EU in the context of ECRIS TCN have the following characteristics:
    - the fingerprint images are contained in a NIST file compliant with ANSI/NIST-ITL 1-2000;
    - a NIST file contains one set of images of 10 rolled fingers and associated slap (plain) images;
    - the fingerprint images have a resolution of at least 500 dpi and are provided in WSQ image format;

  - the NIST file has a compression rate set around 12:1 and the average size of such a file is 1,5 MB.

- Data retention: it is assumed that the data retention policies for the central system will be managed by Member States based on their national legislation. Therefore it is up to the Member States to apply their retention policies by adding/removing identity records in/from the ECRIS TCN systems. Typically, retention periods for criminal records are long and can go up to 75 years in some cases. For the purpose of this study, it is considered that all data is kept at least for 7 years. This is reflected in the volumes of data described in Annex II and used as basis for the cost estimates.
- Legacy data: the ECRIS TCN systems (both national and central) will need to be able to include all identity records of convicted TCN already stored in all Member States before the entry into force of the ECRIS TCN legislation. It is assumed that the backlog (i.e. upload of legacy data) is done at or shortly after the go-live of the central ECRIS TCN system. For the purpose of this study it is assumed that, by the entry into force of the ECRIS TCN legislation, the Member States will have registered approximately 9,1 million alphanumeric identity records and 3 million fingerprints of convicted TCN.
- Security: it is assumed that the alphanumeric identity information, fingerprint files and images are encrypted at network level when sent through the secured TESTA-ng communication network (i.e. usage of HTTPS and security certificates). Access to the ECRIS TCN systems (both national and central systems) needs to be limited to authorised persons and IT systems, with appropriate controls and monitoring.
- Scalability: the ECRIS TCN systems need to be scalable enough to accommodate the growth of the number of entries of identity records (for both alphanumeric identity records and fingerprints) and in the number of processing operations. It is assumed that the IT systems (especially servers and databases) are designed and set-up in such a way that hardware resources can easily be added when needed (for example using techniques such as virtualisation). The volumes and numbers used in this study for estimating the target technical capacity of the systems (in terms of storage and processing operations) assume that the ECRIS TCN solution will be operating at full technical capacity from the start and that this technical capacity remains stable every year during the period on which the costs are calculated.
- Technical integration: the technical components of the ECRIS TCN systems (both national and central) need to provide technical services (e.g. an API) in such a way that they can be accessed and used programmatically. Indeed, the national ECRIS TCN systems will need to provide technical services to facilitate the integration with other national IT systems (i.e. the criminal record registers and the existing ECRIS applications) and the central ECRIS TCN system will need to provide technical services to be used by the national ECRIS TCN systems. Similarly this study assumes that the existing ECRIS Reference Implementation will also be modified to facilitate the technical integration with the national ECRIS TCN system and the ECRIS-TCN system.

- Environments and installations: this study assumes that for each IT system the set-up, deployment and further maintenance requires several environments and installations. At least the following are systematically foreseen and included in the cost estimates:
    - production environment: environment used for the real live systems and data exchanges;
    - pre-production environment: environment to be used for validation testing purposes. This installation is expected to have the same characteristics as the production environment. In particular it also needs to be connected to the secured TESTA-ng network to allow conducting full connectivity and functional testing with Member States.

  In addition to the environments listed above, it is expected that during the development and maintenance of the IT systems additional development and test environments – with lower specifications than the production and pre-production environments – are set-up and used.

- Availability: The ECRIS TCN systems (both national and central) and their subsystems (in particular the central alphanumeric search engine and central AFIS), should reach no less than 97% of uptime per calendar year. The ECRIS TCN solution is conceived for judicial and administrative purposes, and thus it does not need to be operational 24 hours, 7 days per week, 365 days per year. The basic requirement for the central ECRIS TCN system is to reach the target availability of 97% on a basis of 5 working days per week, during the regular working hours. The Return to Normal Operations (RTO) should not exceed 1 week in case of a major disaster.
- This implies that maintenance activities, upgrades, restarting of servers and databases, back-up procedures, etc. can be reasonably foreseen to take place outside of normal working hours (for example nightly) and/or during week-ends or office closing days. Underlying systems can thus be shut down or rendered inoperative for such maintenance activities.
- In practice, for the underlying IT infrastructure and design of the applications it means that:
    - It is not necessary to foresee systematic duplication/redundancy of all physical components (servers, databases, etc.) and data for having live fail-over systems in case of unexpected downtimes of the primary systems.
    - Clustering and load balancing are not strictly mandatory but only need to be set-up if they are necessary for meeting the target response times for the expected load. This being stated, it is assumed that the ECRIS TCN systems are in any case designed in such a way that they can support clustering and load balancing if needed.
    - Data back-ups can be done offline (i.e. 'cold' backups). It is assumed that back-ups are taken regularly (i.e. every night) and the backed up data is kept physically separately from the production servers so as to avoid permanent loss of data.

3.3.2 Characteristics of the national ECRIS TCN system

This section describes the functions to be provided by the national ECRIS TCN system for supporting the ECRIS TCN business processes:

- Storing and updating alphanumeric identity and fingerprint records of TCN received from the criminal records register.
- Extracting alphanumeric identity information possibly contained in the NIST files received as input.
- For each alphanumeric identity record and for each set of fingerprints, storing additional metadata provided together with the record by the criminal records register (e.g. unique technical reference of the record as known at national level, possibly dates/timestamps, etc.).
- Uploading new and modified alphanumeric identity and fingerprint records to the central ECRIS TCN systems. These uploads are expected to be incremental, meaning that only changes since the last upload are sent to the central system.
- Performing the 'hit/no hit' search by automatically querying the central ECRIS TCN system, using alphanumeric identity information and fingerprints received as input.
- Generating a draft ECRIS request message based on the list of Member States with hits received as response from the 'hit/no hit' search and automatically uploading it into the ECRIS systems installed at national level.
- Retrieving and providing as output the identity records (alphanumeric and fingerprints) stored internally, based on the technical references provided.
- Deleting alphanumeric identity and fingerprint records previously stored, and propagating the deletion of identity records to the central ECRIS TCN system.

3.3.3 Characteristics of the central ECRIS TCN system

This section describes the functions to be provided and requirements to be met by the central ECRIS TCN system for supporting the ECRIS TCN business processes.

3.3.3.1 Functions of the central ECRIS TCN system

The following functions need to be provided by the central ECRIS TCN system:

- Storing and updating alphanumeric identity records of TCN in such a way that they can be used for *fuzzy searching* with the highest possible level of accuracy.
- Verifying the quality of fingerprint data in the NIST files uploaded by the national ECRIS TCN systems for storage, and returning comprehensive errors in case the target quality thresholds are not met.
- Storing and updating fingerprint records in such a way that they can be used for *one-to-many matching* with the highest possible level of accuracy.
- Deleting alphanumeric and biometric identity records previously stored, at the instigation of the Member State which provided the data.

- For each alphanumeric identity record and for each set of fingerprints, storing additional metadata provided together with the record by the convicting Member State (e.g. the code of the convicting Member State, unique technical reference of the record as known at national level, possibly dates/timestamps, etc.).
- Performing a 'hit/no hit' search based on the following logic:
    - The central ECRIS TCN system receives as input alphanumeric identity records (can be multiple records, including possible alias identities or name variations) and one NIST file containing one set of fingerprint images. It is assumed that fingerprint images received as input were captured in controlled environments and with the same level of quality as the ones that are uploaded upon convictions of TCN for storage at central level.
    - The system triggers internally the following parallel searches: a *fuzzy search* performed by the internal alphanumeric search engine based on the received alphanumeric identity records and a *one-to-many search* performed by its AFIS using the received set of fingerprints.
    - Each subsystem performs the matching using its own set of algorithms and returns hits or no hits. In case of hits, the information returned may include the corresponding identity information stored in the central ECRIS TCN system. The response also needs to include the metadata that was associated with the record that triggered the hit (e.g. the code of the convicting Member State, the national unique technical reference associated with the record, etc.).
    - The results of the 2 internal search processes is consolidated into a single list of hits, or no hit, together with the identity information where requested, and the response is provided to the national ECRIS TCN system that triggered the search.
- At this stage, the details for the matching algorithms of the alphanumeric search engine are not known. However, having the search engine only perform an exact match on the first and last names provided would not yield correct results in the context of ECRIS TCN: given the known difficulties for identifying TCN using alphanumeric information only it is expected that it would only rarely return hits (i.e. too many 'false negatives'), rendering the system completely inefficient. This study assumes thus that the search engine will be based on various fuzzy logic algorithms, and even possibly combinations of several algorithms, such as:
    - usage of approximations of names, based on common spelling mistakes in names depending on dictionaries per origin of the name (e.g. Lee = Li = Ly, Omar = Umar = Omer, etc.);
    - usage of internal dictionaries of commonly used translations and transformations of names (e.g. Marie = Mary, Bob = Robert, etc.);
    - transliteration of names from non-Roman script to Roman script and vice-versa;
    - phonetic matching algorithms;

  - storage and usage of normalized forms of names used as indexes for searching (e.g. replacing accentuated characters, avoiding special characters, etc.). Example of a common pattern: "Van d'Hervé" is normalised as "VAN D HERVE" for the purpose of matching;
  - cross-referencing of the matches with the other metadata such as date of birth (e.g. comparison of year only, then comparison of year and month, then full comparison place of birth, parent's names, identification documents etc.).
- Limiting the access to the exposed technical services to authorised systems only (including handling of access control rules and regular monitoring of usage/accesses).
- Providing necessary house-keeping and administration features for the proper operational management and maintenance by eu-LISA (e.g. monitoring logs, verifying stability and availability of system, raising alerts in case of serious issues, etc.).
- Providing metrics, statistics and reports on the usage of the system (e.g. number of 'hit/no hit' search queries performed, number of searches with 'hits' or 'no hit', number of identity records stored per country, number of errors that occurred during a period of time, etc.).
- Duplication checks are not required in the context of ECRIS TCN. When registering a set of fingerprints, the internal AFIS must not perform checks for duplicates. Having multiple sets of fingerprints referring to the same individual is actually wanted and expected in the context of ECRIS TCN. Indeed, when considering recidivism and mobility of criminals, it is possible that the same person is convicted multiple times in different Member States at different moments. This leads to different sets of fingerprints being captured in the convicting Member States for the same person.
- Deduplication of NIST files is understood as a technical process that verifies whether a given NIST file contains multiple images of the same finger(s). Concerning the central ECRIS TCN system there is no hard requirement concerning deduplication. Indeed, it is considered the responsibility of Member States to verify this before trying to upload NIST files into the ECRIS TCN systems. It is however expected that before each upload of a new set of fingerprints the system verifies the quality of the proposed NIST file. Amongst the quality verifications performed it is assumed that the central ECRIS TCN system verifies whether there are multiple images of the same finger(s) inside the NIST file and that it outputs a corresponding warning or error code.

3.3.3.2 Technical characteristics of the central ECRIS TCN system

This section presents the system requirements and technical characteristics assumed for the central ECRIS TCN system:

- Restore time: the central ECRIS TCN system (including the alphanumeric search engine and AFIS subsystems) should be considered an 'Essential' system per the classification of European Commissions systems (SEC(2006)898 and SEC(2006)899). This implies that the Return to Normal operations (RTO) should not exceed 1 week.

- Data loss: the central ECRIS TCN system installation in the production environment is assumed to be backed up regularly to avoid permanent loss of data. For the purpose of estimating the costs, it is assumed that regular backing up of all the subsystems, including the storage of alphanumeric identity records and back-up of the fingerprint data stored in the AFIS, is performed. The back-ups are taken at least once per day (typically they could be scheduled nightly).
- Accuracy: the matching accuracy needs to be as high as technically possible for the central ECRIS TCN system. This is a key requirement as it is critical for the overall success of the central ECRIS TCN system. The following objectives need to be reached:
    - The accuracy for the *fuzzy search* based on alphanumeric identity records needs to be as high as technically possible. While ECRIS TCN puts emphasis on the usage of fingerprints, in practice it is expected that many 'hit/no hit' search queries will still be done solely based on alphanumeric identity information.
    - Regarding the *one-to-many matching* using fingerprints, the matching accuracy also needs to be as high as technically possible. Primarily the system must return the fewest possible false-positive hits (i.e. wrong hits). Indeed, too many regular false-positive hits would render the system completely unusable for Member States as they would systematically be spammed by ECRIS requests for which no response can be provided. In a second step, it is also assumed that additional effort is spent for reducing as much as technically possible the number of false-negatives (i.e. missing hits), without affecting the very high accuracy of false-positive hits.
- Response times: the time to get the response from a 'hit/no hit' search query is not business critical. Between the moment that a user initiates the 'hit/no hit' matching process and results are provided, it is considered acceptable to wait up to 1 hour at most for the response. This comes from the fact that responding to an ECRIS request is a business process that takes several days (i.e. 10 working days in most cases, and up to 20 working days under specific conditions). The target response times must however be guaranteed while the system handles a high number of parallel processing operations.

3.4 Main changes to the existing ECRIS systems

The ECRIS systems currently work on the basis that a request for information on past conviction is always sent to the country of nationality of the person. An ECRIS request is thus always sent to one Member State and one response is expected (with or without convictions). To support requests for TCNs, the ECRIS mechanisms will need to be adapted to allow sending the same ECRIS request to multiple Member States and collecting several responses asynchronously while consolidating them into a single response showing all information on past convictions received.

This study thus foresees costs for changing the detailed technical specifications of ECRIS and for upgrading the ECRIS Reference Implementation (including analysis, development, testing, deployment, support and maintenance).

4 Estimated costs for the centralised ECRIS TCN solution

This section presents the cost assessment and the analysis of the technical and operational impact of establishing a centralised ECRIS TCN solution. The section also outlines the main assumptions taken into account to estimate the costs of implementing the centralised ECRIS TCN solution.

4.1 General cost assessment assumptions

The cost assessment of the establishment of a centralised ECRIS TCN solution takes into account several assumptions. Assumptions specific to each cost item composing the solution are presented together with the detailed cost item description (section 4.2). The following points describe general cost assumptions applied to all cost estimates presented in this study.

- Costs for using the TESTA-ng communication network – Currently the exchange of criminal record data among Member States is performed through ECRIS using the TESTA-ng network[51]. TESTA-ng is the European Community's own private network enabling data exchange between Member States, EU Institutions and EU Agencies. This network provides e-communication services for data exchanges required for the implementation of any European policy. In this study we assume that the existing TESTA-ng communication access point and bandwidth currently deployed in Member States and used in the context of ECRIS would be reused for the central ECRIS TCN system. Moreover, this study assumes that the bandwidth increase due to the exchanges of fingerprints does not represent an incremental cost incurred for the use of TESTA-ng communication network for the ECRIS TCN exchanges.
- Timeline: The costs assessed in this study account for three years project implementation and six years of system operation. More specifically, it is assumed that the solution will be implemented in 2018, 2019 and 2020 including 1 year for procurement process, 1,5 year for system development, and 0,5 year for testing the system. It is important to note, that the project implementation can start only after the ECRIS TCN legal text is legally adopted. Following the implementation, this study accounts for the costs incurred during six year of operation (i.e. 2021, 2022, 2023, 2024, 2025 and 2026).
- Data sources and data extrapolation – The cost assessment is based on data collected from Member States[52], eu-LISA[53], AFIS vendors[54], search engine software vendors, ECRIS technical experts, desk research and benchmarking with similar technical solutions (e.g. ECRIS, EEAP,

[51] European Criminal Record Information System (ECRIS), Technical Specifications (TS), Reference Implementation (RI), Information on ECRIS and ECRIS RI, DG JUST, Brussels, April 2015.

[52] Kurt Salmon's online questionnaire, August 2015. 11 Member States provided reliable cost data. The missing data was substituted based on the assumptions and data extrapolation. Detailed description can be found in Annex III.

[53] Wavestone data collection activities with eu-LISA, March 2017. Detailed cost information was provided. More information regarding each individual cost item is presented in Annex III

[54] Wavestone interviews conducted with AFIS vendors, April 2017.

etc.). Data extrapolation techniques were used whenever data was missing or data was considered inconsistent. Annex III details the data source and the data extrapolation technique applied to each cost item.

- Round of numbers – This study applies the general recommendations[55] of Eurostat for rounding of numbers. Rounding was performed at the latest phase of data processing and analysis. In order to facilitate the reading of figures, all cost estimates presented in tables are rounded to thousands and all cost estimates presented in figures are rounded to millions. Due to rounding, some totals may not correspond with the sum of the individual figures.
- Assessed costs – According to the Better Regulation Guidelines[56] and the Better Regulation Toolbox[57] this ICT Assessment assesses the substantive compliance costs (i.e. incremental costs). The substantive compliance costs encompass the incremental (i.e. non business as usual) costs to the target group of complying with the regulation other than fees and administrative costs. The assessed substantive compliance costs according to the ICT cost categories specified in the Better Regulation Toolbox are as follows:
  - Hardware costs – provide the total (anticipated) cost of the hardware (e.g. network, servers) required to develop, support, operate and maintain the system. Hardware costs are accounted as one-off costs (i.e. investment costs related to the establishment of the system) and as ongoing costs (i.e. recurring cost for the maintenance of the hardware, including replacement of the hardware).
  - Software costs – provide the total (anticipated) cost of software (e.g. applications, libraries) required to develop, support, operate and maintain the system. Software costs are accounted as one-off costs (i.e. investment costs related to the establishment of the system) and as ongoing costs (i.e. recurring cost for the maintenance of the software, including upgrades).
  - Development costs – provide the total (anticipated) cost (human resources and other) for the development of the system (e.g. analysis and process reengineering activity, coding activity, project management activity, test activity, configuration & change management activity, deployment activity). Development costs are accounted as one-off costs (i.e. investment costs related to the establishment of the system).
  - Maintenance costs – provide the total (anticipated) cost (human resources and other) in person days per year to maintain the system (e.g. activities related to both corrective maintenance and evolving maintenance). Maintenance costs are accounted as ongoing costs (i.e. incremental recurring costs of operation of the system).
  - Support costs – provide the total (anticipated) cost (human resources) in person days per year to support the system (e.g. helpdesk, operations). Support costs are accounted as ongoing costs (i.e. incremental recurring costs of operation of the system).

[55] Eurostat tutorial on rounding of numbers.
[56] Better Regulation Guidelines [COM (2015)205 final] European Commission, 19.05.2015.
[57] Better Regulation Toolbox #23 ICT Assessment, The Digital Economy and Society SWD(2015) 111 final, European Commission, 19.5.2015.

- Technology upgrade – The system is not expected to be upgraded before the first six years of operation (i.e. 2021, 2022, 2023, 2024, 2025, and 2026). Therefore, regarding the upgrade of the system, this study only accounts for evolving and corrective maintenance costs and the ongoing software and hardware costs (i.e. software upgrades and replacement of broken, used, obsolete hardware).
- Labour Daily Rates – costs collected in person days[58] were converted into costs (monetary figures) using the labour daily rates to convert person days into Euros.
  - For cost items incurred by Member States: the persons days estimates collected from Member States are computed using the labour daily rates provided by Eurostat's hourly labour costs for 2015[59] to convert person days into Euros.
  - For cost items incurred by European Union: regarding development work of a contractor at central level, a 500 EUR person day is used to monetise the effort. Table 2 below present the Full Time Equivalent (FTE) values used for calculating the effort for maintenance, support and coordination.

Table 2 Full Time Equivalent values

Staff category	Yearly cost including office space and furniture (in euro)
Commission Official (FTE)	138 000
Temporary agent (FTE)	138 000
National Expert (FTE)	78 000
Contract Agent (FTE)	70 000

Source: European Commission's Directorate-General for Justice and Consumers (DG JUST), April 2017.

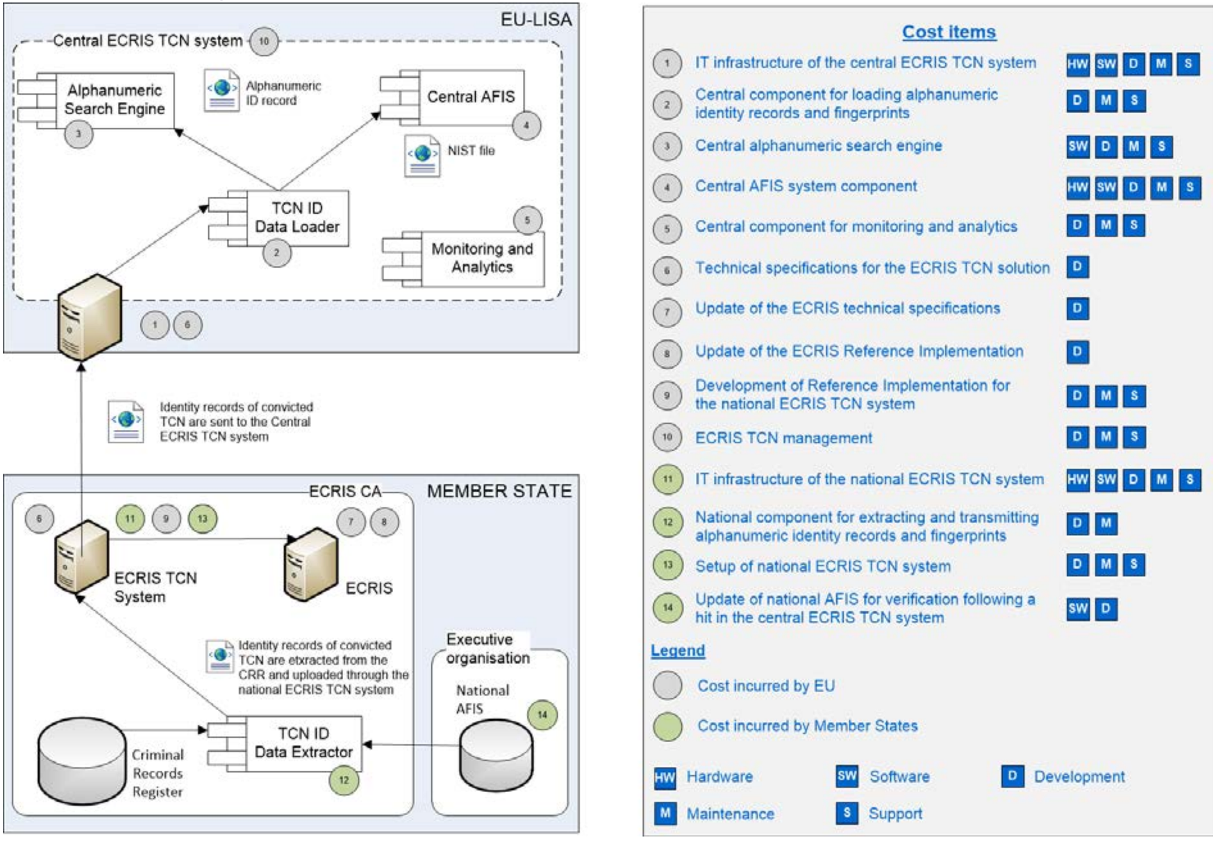
4.2 Cost assessment: centralised ECRIS TCN solution

This section provides the description, assumptions and cost estimations related to the cost items comprising the *centralised ECRIS TCN solution* as depicted in Figure 11.

[58] This includes costs collected in fraction of a day, hours and minutes.

[59] The labour daily rates are based on an 8 hour working day and an average hourly labour costs which are defined as total labour costs divided by the corresponding number of hours worked by the yearly average number of employees, expressed in full-time units. Labour Costs (D) cover Wages and Salaries (D11) and non-wage costs (Employers social contributions plus taxes less subsidies: D12+D4-D5).

Figure 11 Centralised ECRIS TCN solution: Architecture and cost items


EU-LISA
Central ECRIS TCN system 10
Alphanumeric Search Engine 3
Alphanumeric ID record
Central AFIS 4
NIST file
TCN ID Data Loader 2
Monitoring and Analytics 5
1 6
Identity records of convicted TCN are sent to the Central ECRIS TCN system
MEMBER STATE
ECRIS CA
6
11 9 13
7 8
ECRIS TCN System
ECRIS
Identity records of convicted TCN are etxracted from the CRR and uploaded through the national ECRIS TCN system
Executive organisation
National AFIS 14
Criminal Records Register
TCN ID Data Extractor 12
Cost items
1 IT infrastructure of the central ECRIS TCN system HW SW D M S
2 Central component for loading alphanumeric identity records and fingerprints D M S
3 Central alphanumeric search engine SW D M S
4 Central AFIS system component HW SW D M S
5 Central component for monitoring and analytics D M S
6 Technical specifications for the ECRIS TCN solution D
7 Update of the ECRIS technical specifications D
8 Update of the ECRIS Reference Implementation D
9 Development of Reference Implementation for the national ECRIS TCN system D M S
10 ECRIS TCN management D M S
11 IT infrastructure of the national ECRIS TCN system HW SW D M S
12 National component for extracting and transmitting alphanumeric identity records and fingerprints D M
13 Setup of national ECRIS TCN system D M S
14 Update of national AFIS for verification following a hit in the central ECRIS TCN system SW D
Legend
Cost incurred by EU
Cost incurred by Member States
HW Hardware
SW Software
D Development
M Maintenance
S Support

Source: WAVESTONE Feasibility study and cost assessment of the establishment of a centralised ECRIS TCN solution, June 2017

Table 3 presents a tabular view of the description, assumptions and cost estimates per cost item incurred by the European Union.

Table 3 Centralised ECRIS TCN solution: Costs incurred by the European Union

Costs incurred by the European Union (*in million EUR, to three decimal places)*	One-off costs (3 years)	Ongoing costs (1 year)
1 – IT infrastructure of the central ECRIS TCN system • Description: This cost item includes the acquisition, installation and configuration of the required hardware (e.g. database servers, application servers, virtualisation servers, management servers, racks, etc.) and COTS (Commercial Off the Shelf) software for running the centralised ECRIS TCN system. The cost item also includes the operational ongoing costs for hardware, software, maintenance and support (helpdesk) of the overall IT infrastructure. The cost item does not account for costs related to the central AFIS system (see cost item 4). • Assumptions: The following is assumed: o Availability – 97%, 10 hours/day during working hours and 5 days a week. o Restore time - Return to Normal operations (RTO) should not exceed 1 week o Response time - The time to get the response from the 'hit/no hit' search is not critical. It is acceptable to wait up to 1 hour at most for the response. o Software and Hardware cost accounts for production and pre-production environments of a Central Unity (CU).	1,498	0,285

Costs incurred by the European Union (*in million EUR, to three decimal places)*	One-off costs (3 years)	Ongoing costs (1 year)
2 – Central component for loading alphanumeric identity records and fingerprints • Description: This cost item includes the development and maintenance and support (helpdesk) of a technical component which loads alphanumeric identity records and fingerprints received from Member States into the central ECRIS TCN system. The functionalities addressed by this component include: o The incremental insert / delete / update records; o The initial data load (backlog/migration) of the alphanumeric and biometric identity records currently stored by Member States in their national systems; o Quality control of identity records data received by the national ECRIS TCN systems. • Assumptions: It is assumed that: o This component will be integrated in the central ECRIS TCN system; o The initial data load will be performed through a web interface that can be used for uploading very large datasets in bulk mode; o Member States will ensure the conversion of the data (i.e. alphanumeric identity records and fingerprints) into an ECRIS TCN standard format.	0,200	0,025
3 – Central alphanumeric search engine • Description: This cost item includes the software licenses and development effort for integrating an alphanumeric search engine in the central ECRIS TCN system. Specific requirements for the search engine are described as part of the technical specification (cost item 6). This cost item also accounts for maintenance and support (helpdesk) of the central alphanumeric search engine software. • Assumptions: It is assumed that this cost estimate includes the purchase of a dedicated license for a search engine.	1,990	0,340
4 – Central AFIS system component • Description: This cost item consists of the implementation of a dedicated AFIS system component contained within the central ECRIS TCN system. The AFIS component should provide features such as: o Compliance and quality checks of the NIST files and fingerprints provided by Member States; o Storage of fingerprint records (original NIST file + fingerprint templates); o One-to-many matching of fingerprints. This cost item also accounts for maintenance and support (helpdesk) of the central AFIS system component. • Assumptions: It is assumed that the central AFIS system component would be able to cope with the volumes of searches and storage expected in the ECRIS TCN solution.	5,100	0,720
5 – Central component for monitoring and analytics • Description: This cost item consists of configuration, maintenance and support (helpdesk) of a technical component within the central ECRIS TCN system responsible for monitoring its use by collecting metrics and producing reports. For example: o Monitor the provision of identity data records by the Member States to the central ECRIS TCN system (traceability/audit mechanism to allow tracking of who has provided which data and when it was provided); o Monitoring and providing statistics reports on the hit/no-hit searches. The cost item does not account for costs related to hardware and COTS software costs which are accounted under cost item 1. • Assumptions: It is assumed that: o 25 reports of average complexity will be developed as part of this cost item using a middleware such as Crystal reports; o No dedicated database tables are expected to be used other than the one used in the transactional tables of the central ECRIS TCN system.	0,150	0,030

Costs incurred by the European Union *(in million EUR, to three decimal places)*	One-off costs (3 years)	Ongoing costs (1 year)
6 – Technical specification for the ECRIS TCN solution • Description: This cost item consists of the development of the detailed technical specifications (documentation) for the ECRIS TCN solution. The technical specifications aim at guiding the overall implementation of the national ECRIS TCN systems in Member States. These specifications would include: o Specification of the technical interfaces for integration of the national ECRIS TCN system with ECRIS, CRR, and the central ECRIS TCN system; o Specification of the data structure and NIST files to be provided by Member States; o Specification of the quality levels and thresholds for TCN fingerprints. • Assumptions: It is assumed that the maintenance of the technical specifications is included in the overall maintenance of the ECRIS TCN solution, accounted under cost item 10.	0,190	-
7 – Update of the ECRIS technical specifications • Description: This cost item consists of the update of the existing detailed technical specification (documentation) of ECRIS in order to accommodate the changes added due to the new components of the ECRIS TCN solution. These technical specifications are documents that enable Member States to develop and maintain their own implementation of ECRIS. • Assumptions: It is assumed that the maintenance of the ECRIS technical specifications is part of the ECRIS project, therefore it is not accounted as part of the support and maintenance of the ECRIS TCN solution.	0,067	-
8 – Update the ECRIS Reference Implementation • Description: This cost item consists of updating the current ECRIS Reference Implementation in order to build the capacity to integrate with the national ECRIS TCN system and to apply the ECRIS TCN principles (one-to-many ECRIS requests for TCN). • Assumptions: It is assumed that the regular support and maintenance of the ECRIS RI is part of the ECRIS project, therefore it is not accounted as part of the support and maintenance of the ECRIS TCN solution.	0,259	-
9 – Development of Reference Implementation for the national ECRIS TCN system • Description: This cost item consists of the development, maintenance and support (helpdesk) of a Reference Implementation for the national ECRIS TCN system. This includes: o Technical interfaces for integration of the national ECRIS TCN system with the CRR and with ECRIS; o Technical interface with the central ECRIS TCN system. o Application for sending updates on inclusion/removal of identity data to the central AFIS; o Application for sending search queries to the central ECRIS TCN system and collect results. • Assumptions: The following is assumed: o Member States will be able to use the Reference Implementation; o Additional cost on opting for a national implementation is not a cost mandated by the legislation.	1,046	0,209

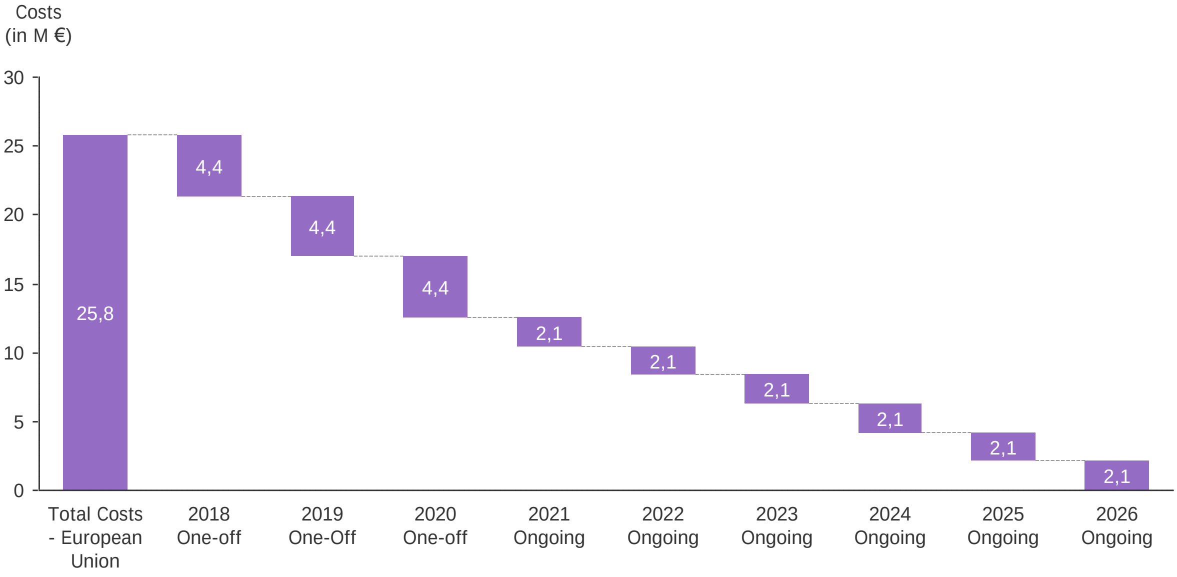
Costs incurred by the European Union (*in million EUR, to three decimal places)*	One-off costs (3 years)	Ongoing costs (1 year)
10 –ECRIS TCN management • Description: This cost item includes the effort required for the following activities: o Governance and administration (e.g. legal, procurement, coordination with Member States etc.). o Project and change management. o Organisation of meetings during development and operation. o Technical maintenance and support (e.g. application management, system administration, network, etc.). • Assumptions: It is assumed that a number of 18 advisory group meetings and 8 comitology meetings will be held for a period of nine years (i.e. three years implementation and six years operations).	2,762	0,476
Total costs: European Union	13,262	2,085

Source: WAVESTONE Data Analysis, April 2017.

As shown in Table 3 above, the total one-off costs incurred by the European Union to implement the centralised ECRIS TCN solution are approximately EUR 13 million over a time period of three years and the total ongoing costs are approximately EUR 2 million per operating year.

Figure 12 below presents a waterfall visualisation of the total estimated cost incurred by the European Union for implementing the *centralised ECRIS TCN solution* for a period of nine years (i.e. 3 years one off costs and 6 years ongoing costs).

Figure 12 Centralised ECRIS TCN solution: Nine-year total costs incurred by the European Union



Source: WAVESTONE Data Analysis, April 2017.

The total costs incurred by the European Union for a period of nine years are approximately EUR 26 million. Table 4 below presents a tabular view of the description, assumptions and cost estimates per cost item incurred by the 28 Member States.

Table 4 Centralised ECRIS TCN solution: Costs incurred by the 28 Member States

Costs incurred by the 28 Member States (*in million EUR, to three decimal places*)	One-off costs (3 years)	Ongoing costs (1 year)
11 – IT infrastructure of the national ECRIS TCN system • Description: This cost item includes the acquisition, installation and configuration of the required hardware (e.g. servers, racks, etc.) and COTS software (Commercial Off the Shelf) for running the national ECRIS TCN system. The cost item also includes the ongoing maintenance and support costs of the national ECRIS TCN system. • Assumptions: The following is assumed: o The TESTA-ng communication network, already used in ECRIS, will be reused. Therefore no incremental costs are accounted for network. o All COTS software used to run the national ECRIS TCN Reference Implementation are open software. Therefore no incremental costs are accounted for software.	0,514	0,152
12 – National component for extracting and transmitting alphanumeric identity records and fingerprints • Description: This cost item includes the development and maintenance of a component of the national criminal records register (e.g. routine/script) that will automatically and regularly extract identity records and fingerprints from the national criminal records register and transmit them to the national ECRIS TCN system. The national ECRIS TCN system is then responsible for transmitting the data to the central ECRIS TCN system. • Assumptions: It is assumed that the extraction of identification data from the national criminal records register is performed automatically, for example by means of web services. The extraction is assumed to be of low complexity for all Member States. This assumption is based on the fact that all Member States: o Store electronically the same alphanumeric information on convicted TCN as on convicted EU nationals; o Store electronically the criminal record information on TCN in the same national register as for EU nationals; and o Store electronically the criminal record information on TCN in a single (central) database.	0,342	0,075
13 – Setup of the national ECRIS TCN system • Description: This cost item consists of the installation, configuration, maintenance and support of the national ECRIS TCN system. This includes: o Installing the national component for extracting and transmitting alphanumeric identity records and fingerprints; o Installing the ECRIS TCN Reference Implementation in the Member States premises; o Installing and testing the integration between the ECRIS TCN Reference Implementation and ECRIS; o Configuring the ECRIS Reference Implementation, the ECRIS TCN Reference Implementation and the national component for extracting and transmitting alphanumeric identity records and fingerprints; o Interconnecting the ECRIS Reference Implementation, ECRIS TCN Reference Implementation, the national component for extracting and transmitting alphanumeric identity records and fingerprints, with the CRR and national AFIS; o Connecting the national ECRIS TCN Reference Implementation system with the central ECRIS TCN system. • Assumptions: It is assumed that the fingerprints used in the national ECRIS TCN system are available in the national AFIS. Given the expected complexity of interconnecting the several components of the ECRIS TCN system, it is assumed that this work will be done by specialised contractors.	3,500	1,260

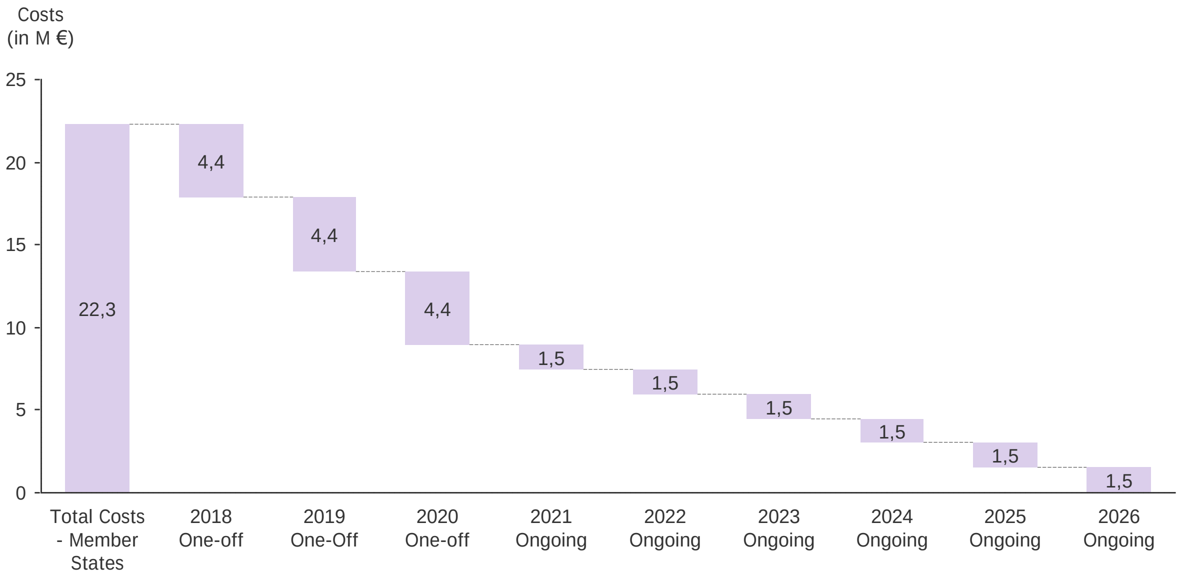
Costs incurred by the 28 Member States (*in million EUR, to three decimal places)*	One-off costs (3 years)	Ongoing costs (1 year)
14 – Update of national AFIS for verification following a hit in the central ECRIS TCN system • Description: This cost item consist of upgrading the national AFIS as follows: in case of a "hit", upon a request of a Member State, the requested Member State might decide to perform a verification at national level, using an existing AFIS, based on fingerprints transmitted with the request. • Assumptions: It is assumed that: o The requested Member States will use an existing national AFIS to perform the verification process. Therefore this cost item includes the incremental development and software costs for upgrading the national AFIS. o There are no incremental hardware, maintenance and support due to the reuse of existing AFIS at national level. o Work would be performed by specialised contractors (e.g. AFIS experts).	8,988	-
Total costs: 28 Member States	13,344	1,487

Source: WAVESTONE Data Analysis, April 2017.

As shown in Table 4, the total one-off costs incurred by the 28 Member States to implement the centralised ECRIS TCN solution are approximately EUR 13 million over a time period of three years and the total ongoing costs are approximately EUR 1,5 million per operating year.

Figure 13 below presents a waterfall visualisation of the total estimated cost incurred by the Member States for implementing the *centralised ECRIS TCN solution* for a period of nine years (i.e. 3 years one off costs and 6 years ongoing costs).

Figure 13 Centralised ECRIS TCN solution: Nine-year total costs incurred by the 28 Member States



Source: WAVESTONE Data Analysis, April 2017.

The total costs incurred by the 28 Member States for a period of nine years are approximately EUR 22 million. Table 5 below summarises the total costs incurred by the European Union and by the Member States to implement the *centralised ECRIS TCN solution* for a period of nine years.

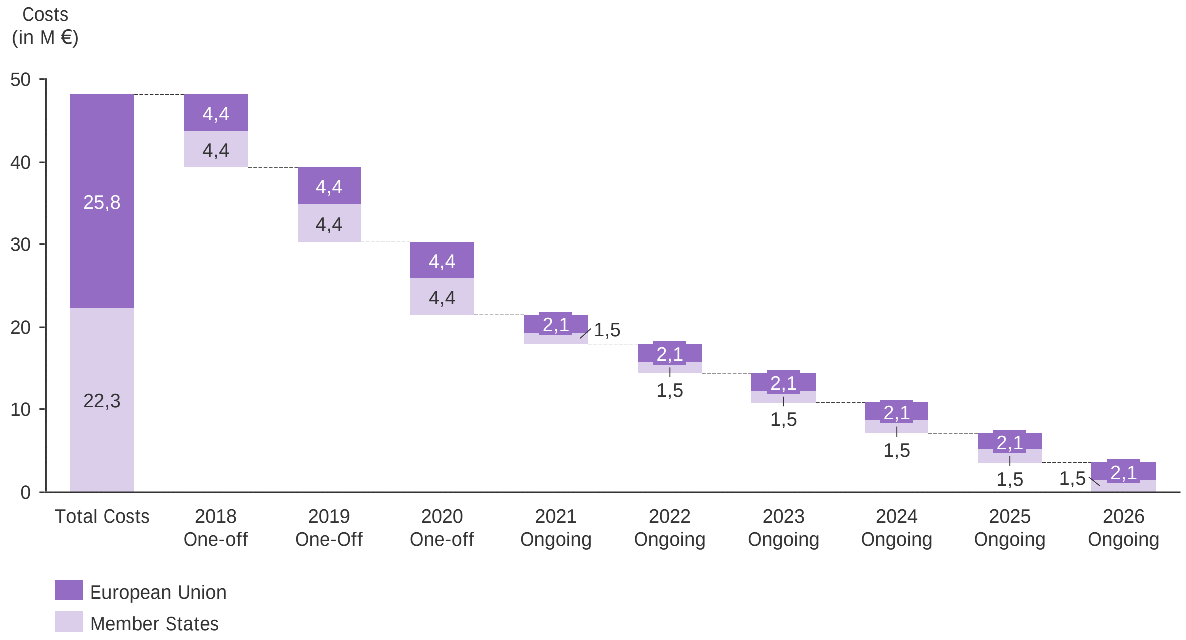
Table 5 Centralised ECRIS TCN solution: Total costs summary[60]

Estimated total costs (*in million EUR, to three decimal places)*	2018	2019	2020	2021	2022	2023	2024	2025	2026	Total
Total one-off costs for the European Union	4,421	4,421	4,421	-	-	-	-	-	-	13,262
Total one-off costs for the 28 Member States	4,448	4,448	4,448	-	-	-	-	-	-	13,344
Total one-off costs	8,869	8,869	8,869	-	-	-	-	-	-	26,606
Total ongoing costs for the European Union	-	-	-	2,085	2,085	2,085	2,085	2,085	2,085	12,509
Total ongoing costs for the 28 Member States	-	-	-	1,487	1,487	1,487	1,487	1,487	1,487	8,920
Total ongoing costs	-	-	-	3,571	3,571	3,571	3,571	3,571	3,571	21,429
Total costs for the European Union	4,421	4,421	4,421	2,085	2,085	2,085	2,085	2,085	2,085	25,771
Total costs for the 28 Member States	4,448	4,448	4,448	1,487	1,487	1,487	1,487	1,487	1,487	22,264
Total costs	8,869	8,869	8,869	3,572	3,572	3,572	3,572	3,572	3,572	48,035

Source: WAVESTONE Data Analysis, April 2017.

Figure 14 below shows the spread between the costs incurred by the European Union and by the 28 Member States for a period of nine years.

Figure 14 Centralised ECRIS TCN solution: Total costs summary



Source: WAVESTONE Data Analysis, April 2017.

Finally, Table 6 presents a consolidated view on the one-off and yearly ongoing costs incurred by the European Union and by the 28 Member States for the implementation of the centralised ECRIS TCN

[60] Due to rounding, some totals may not correspond with the sum of the individual figures.

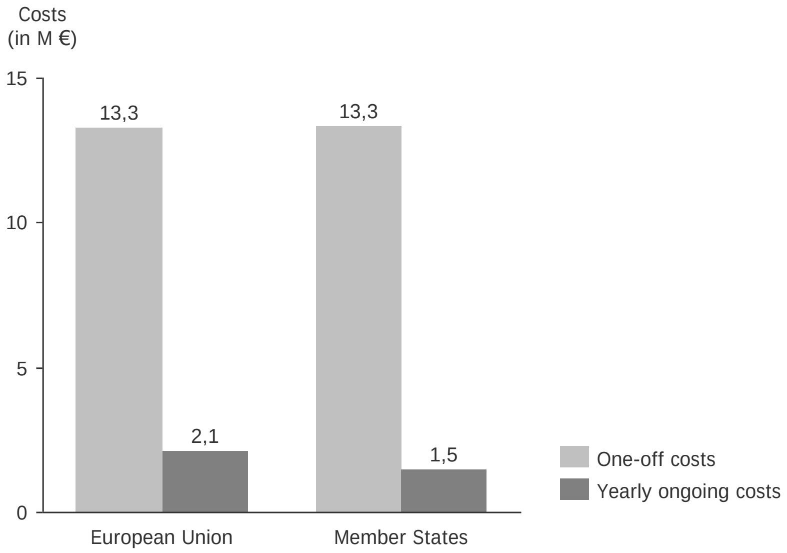
solution. While Table 5 presents the figures on the implementation of the centralised ECRIS TCN solution assuming a timeline of nine years, Table 6 and Figure 15 highlight the consolidated values of one-off costs and the absolute yearly ongoing costs.

Table 6 Centralised ECRIS TCN solution: One-off and ongoing costs

Estimated total costs *(in million EUR, to three decimal places)*	One-off costs	Yearly Ongoing Costs
Centralised ECRIS TCN solution		
European Union	13,262	2,085
Member States	13,344	1,487
Total	26,606	3,572

Source: WAVESTONE Data Analysis, March 2017.

Figure 15 ECRIS TCN: One-off and yearly ongoing costs



Source: WAVESTONE Data Analysis, March 2017.

5 Interoperability and future-proofing of the centralised ECRIS TCN solution

This section elaborates on the feasibility and cost impacts of ensuring the interoperability and future-proofing of the centralised ECRIS TCN solution taking into account the possibilities of using the solution for a broader audience or to make it available to other stakeholders.

5.1 Integration with other large-scale EU systems

This section focuses on providing considerations about the possible future integrations of the centralised ECRIS TCN solution (as described in section 3) with other large-scale EU systems.

5.1.1 Functional, operational and legal considerations

As described in section 3, the solution proposed for ECRIS TCN relies on the centralisation of the identity records of convicted TCN, including fingerprints. The most obvious and direct means for integration would thus be that other large-scale EU systems connect to the central ECRIS TCN system. However, the central ECRIS TCN system does not contain information on the convictions that triggered the registration. A connected system thus cannot automatically know from the central ECRIS TCN system the severity or type of offence for which the registered person has been convicted. In addition, the searches in the central ECRIS TCN system cannot provide absolute certainty on the identity of a person registered. This is due to the fact that recorded names are not necessarily correct and fingerprint matching, although very accurate, cannot guarantee 100% certainty. Thus, the only information that can be retrieved from the central ECRIS TCN system is that a given person was ‛possibly’ convicted in the indicated Member State(s).

For the reasons mentioned above, data exchanges between any other EU system and the central ECRIS TCN system would need to be followed by additional information exchanges with the ECRIS Central Authorities. Such additional information exchanges would first need to be clearly identified and regulated by European and national legislation. This would also put an additional administrative burden on the ECRIS Central Authorities that would need to provide responses to new requesting authorities and for different purposes than the ones foreseen currently in ECRIS. A possibility that could be explored in the future would be to add some information on offences and sanctions in the central ECRIS TCN system, linked to the identity records of the convicted persons (for example the common ECRIS categories of offences and sanctions). Follow-up exchanges of information would still be required in case of a hit to obtain confirmation from the convicting Member State, but the information provided from the central ECRIS TCN system would already give an indication to the requesting authority of the type and severity of the offences possibly committed by the person. This would allow the requestor to judge whether it is indeed relevant to pursue the investigations, and thus minimise the administrative burden. As the centralised ECRIS TCN solution already foresees the technical means for centralising identity records, and considering that information on offences and sanctions are only text records, adding such information in the data exchanges would not be very difficult from a technical point of view. The main issue would be to agree on the legal framework for centralising such type of information and ensure that it would not be misused or misinterpreted.

Another issue to consider is the time needed for obtaining the relevant information. In the ECRIS exchanges, the requested Member State provides the response, possibly containing information on past convictions, within 10 working days (up to 20 working days in specific cases). Such delays are acceptable for the judicial or administrative purposes served by ECRIS but are not acceptable for systems that operate in near real-time, such as border-control systems, where responses need to be provided within seconds. It must be understood that the requested ECRIS Central Authority, in a majority of Member States, needs to perform extensive manual research and cross-verifications at national level for each request received, which explains the time required for providing responses. The only possibility for drastically shortening such processes would be that Member States automate fully the work that is now done manually. This in turn requires the data stored in the national criminal records registers to be fully standardised at national level, to be complete and of very high quality. It also requires additional interconnections at national level for automating verifications that are now done manually (e.g. verifying the identity of the person by cross-checking in other national databases such as social security databases or identity card databases). This is obviously a major difficulty for legacy data and can most probably only be achieved over a long period of time and with considerable investments by the Member States.

5.1.2 Technical considerations

During the analyses carried out for preparing this study, it has been identified that the central ECRIS TCN system has significantly lower requirements in terms of system availability and target response times when compared to other large-scale systems operated and maintained by eu-LISA.

5.1.2.1 Need for high availability

The centralised ECRIS TCN solution is regarded as a judicial-administrative system that needs to operate during office working days and working hours of the national Central Authorities, whereas border management or law enforcement systems typically need to operate and remain available continuously (i.e. 24 hours, 7 days per week, 365 days per year without noticeable interruptions).

This implies that it would be necessary to design the infrastructure of the central ECRIS TCN system so as to also meet high availability requirements in order to realise the technical integration with other large-scale and highly available EU systems. This is technically feasible but has a cost impact. In the case that high availability would be required, the requirements for the central ECRIS TCN system would be typically defined as follows:

- The central ECRIS TCN system, and thus its subsystems including the alphanumeric search engine and AFIS, should reach no less than 99,99% of uptime per calendar year. The central ECRIS TCN system is conceived as a critical system that must remain up and running 24 hours, 7 days per week, 365 days per year. In this scenario, the underlying infrastructure and IT systems need to be conceived and set-up in such a way that, on average, the downtime periods fall within the limits listed in Table 7 below:

Table 7 Requirements for highly available central ECRIS TCN system

Availability %	Downtime per year	Downtime per month	Downtime per week
99.99%	52.56 minutes	4.38 minutes	1.01 minutes

- In order to meet the target requirements for a highly available system, it is assumed that the central ECRIS TCN system would be conceived as follows:
    - Set-up of an active/active architecture that would distribute the user transactions over multiple independent and geographically distributed instances of the system. This involves a systematic duplication of all components (servers, databases, etc.) acting as fail-over systems in case of unexpected downtimes of the primary instances as well as a systematic replication of the data in multiple, separate databases.
    - As the central ECRIS TCN system will be operated by eu-LISA, which already operates other large-scale IT systems, it is assumed that similar high-availability techniques and principles would be used. In particular it is assumed that the instances and data are distributed and replicated across the already existing geographical sites of eu-LISA in Strasbourg (France) and in Sankt Johann im Pongau (Austria).
    - In this case the disaster recovery procedures cannot include the possibility to retrieve the data from the national ECRIS TCN systems; they would rather rely on the fact that the data and processing instances are already systematically replicated in physically remote locations by the active/active architecture.

5.1.2.2 Need for faster response times

As mentioned in the description of the centralised ECRIS TCN solution in section 3, the response times of the IT systems are not a critical factor. It is acceptable that the responses provided by the central ECRIS TCN system for 'hit/no hit' searches take up to 1 hour. However, in case the central ECRIS TCN system needs to be interconnected with other large-scale IT systems that nearly work in real-time, these target response times are largely insufficient. It would thus also be necessary to design the infrastructure of the central ECRIS TCN system so as to provide responses within seconds, consistently and also under high load. In particular this would mean that clustering and load-balancing would need to be set-up from the start so as to meet the target response times for the expected load. Increased costs for the licenses of the AFIS and alphanumeric search products should also be expected in this case, as they will run on a higher number of processing nodes.

It must be noted that the integration with a shared Biometric Matching Service (BMS) would provide a partial solution to the two technical issues on high-availability and response times, at least for the searches on biometrics. By definition and by its nature, the shared BMS will be tailored and designed for meeting requirements on high-availability and faster response times. Section 5.2 details the possible use of a shared BMS in the centralised ECRIS TCN solution. The central ECRIS TCN system would still need to be upgraded for the alphanumeric search engine.

5.1.2.3 Need for higher capacity

At this stage, the number of additional inquiries for searching could not be quantified as the business processes for integration with other large-scale EU systems are unknown. It should be expected however that if that number is significant (i.e. thousands of queries per day), this would necessarily impact the infrastructure, architecture and thus imply a significant increase of the associated costs. This part could however not be estimated in this study.

5.1.3 Cost assessment: highly available central ECRIS TCN system

This section provides the description, assumptions and cost estimations related to the cost items comprising the highly available central ECRIS TCN system. The cost estimates presented in this section are incremental costs that would be incurred by the European Union only if the central ECRIS TCN system would need to comply with the interoperability requirements presented in section 5.1.2. The costs estimates presented in this section should be read by taking into account that these are additional costs to the estimated costs of implementing a centralised ECRIS TCN solution (presented in section 4.2). No incremental costs are foreseen to be incurred by Member States since the changes for a highly available central ECRIS TCN system do not impact the national ECRIS TCN systems. Table 8 presents a tabular view of the descriptions and the incremental costs per cost item incurred by the European Union for the implementation of a highly available central ECRIS TCN system.

Table 8 Highly available central ECRIS TCN system: Incremental costs incurred by the EU

Costs incurred by the European Union (*in million UR, to three decimal places)*	Incremental one-off costs (3 years)	Incremental ongoing costs (1 year)
IT infrastructure of the highly available central ECRIS TCN system • Description: This cost item includes the acquisition, installation and configuration of the additional hardware required (e.g. database servers, application servers, virtualisation servers, management servers, racks CPU nodes, etc.) and additional COTS (Commercial Off the Shelf) software for running the highly available centralised ECRIS TCN system. The cost item also includes the additional operational ongoing costs for hardware and software and support (helpdesk) of the overall IT infrastructure. This cost item does not account for costs related to the highly available central AFIS system. The Infrastructure is designed for higher availability and faster response times, not for the additional load. • Assumptions: o Availability: 99.99% uptime, 24/7 during 365 days per year; o Downtime – Return to Normal operation should not exceed 1.01 minutes per week; o Software and Hardware costs account for production and pre-production environments of a Central Unity (CU) and Back-up Central Unit (BCU).	2,462	0,477
Highly available central alphanumeric search engine • Description: This cost item includes the additional software licenses and development effort for integrating a highly available alphanumeric search engine in the highly available central ECRIS TCN system. Additional requirements for the search engine (e.g. active-active set up, 99.99% availability, etc.) will be described as part of the ECRIS TCN technical specifications. This cost item also accounts for maintenance and support (helpdesk) of the highly available central alphanumeric search engine software.	0,935	0,221

Costs incurred by the European Union (*in million UR, to three decimal places)*	Incremental one-off costs (3 years)	Incremental ongoing costs (1 year)
Highly available central AFIS system component • Description: This cost item consists of the additional costs for the implementation of a highly available dedicated AFIS system as a component contained within the highly available central ECRIS TCN system. This includes additional, hardware, software licenses, maintenance and support costs. • Assumptions: It is assumed that the highly available central AFIS system component would be able to cope with requirements of storage and volume of searches of the ECRIS TCN solution (baseline).	3,140	0,735
Central component for monitoring and analytics (highly available) • Description: This cost item includes the additional configuration and maintenance of a technical component within the highly available central ECRIS TCN system responsible for monitoring its use by collecting metrics and producing reports. This component should cope with the requirements of a highly available ECRIS TCN solution such as active-active architecture. The cost item does not account for costs related to hardware and COTS software costs which are accounted under IT infrastructure of the highly available central ECRIS TCN system.	0,030	0,006
Total costs: European Union	6,567	1,439

Source: WAVESTONE Data Analysis, April 2017.

As shown in Table 8, the total incremental one-off costs incurred by the European Union to implement the highly available central ECRIS TCN system are approximately EUR 6,6 million over a time period of three years and the total incremental ongoing costs are approximately EUR 1,4 million per operating year.

5.2 Use of a shared Biometric Matching Service

The European Commission has designed and implemented a series of large-scale systems in the context of security, border control, travel and migration in which the identification of persons are a key element of the business processes (e.g. the Schengen Information System[61], EURODAC[62], the Visa Information System[63], etc.). Over the years, the use of biometric matching techniques has become a standard practice for providing viable solutions to meet the challenges faced in the identification of persons. In the future, other large-scale systems will need to be implemented and maintained to ensure the safety within the EU, which will also need to use biometric matching techniques. Furthermore there is also a growing need to share the information between systems. The European Commission published in 2016 a Communication[64] assessing the opportunity to create a shared platform that would serve as technical basis for all systems requiring biometric storage and matching services. Such a shared platform would not only serve the specific purposes of each of the systems using it, but would also provide a centralised

[61] Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II).

[62] Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of the Dublin Convention, 11 December 2000.

[63] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), 9 July 2008.

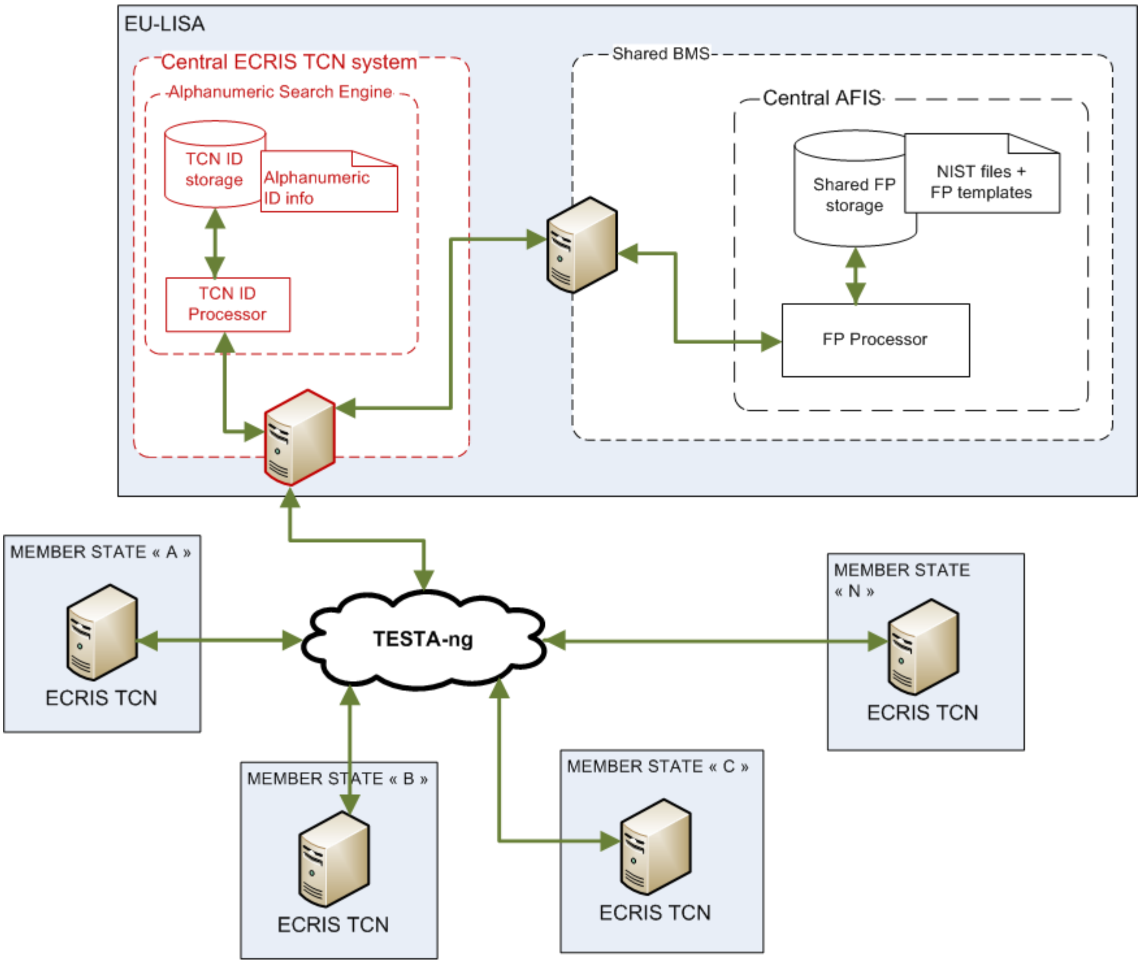
[64] Communication from the Commission to the European Parliament and the Council, Stronger and Smarter Information Systems for Borders and Security, COM(2016) 205 final, Brussels, 6.4.2016.

system in the future that enables the search of persons across the identity records collected throughout the different systems.

Considering that the technical solution envisaged for ECRIS TCN is based on the centralisation of identity records, including fingerprints, it is reasonable to evaluate the possibility to use shared Biometric Matching Services (BMS) for the central ECRIS TCN system rather than setting up a dedicated central AFIS. At the time of writing, DG HOME and eu-LISA were still studying the impacts, technical feasibility and possible scenarios for the establishment of a shared BMS. Even though the conclusions of the shared BMS study are not yet available, a few general considerations can already be made at this stage:

- While the key principles and characteristics of the centralised ECRIS TCN solution would remain identical, the architecture would be different. Figure 16 below illustrates the resulting architecture in case the centralised ECRIS TCN solution is integrated with the shared BMS.
- Although the technical capabilities and features of the shared BMS are unknown at this stage, it can be reasonably assumed that the functions needed by the central ECRIS TCN system (i.e. storage of fingerprints and *one-to-many* matching) will be covered out-of-the-box by the shared BMS as these are basic features provided by all commercial AFIS products. In the context of this study it is assumed that the alphanumeric search engine will still need to be built and designed as a subsystem of the central ECRIS TCN system.
- As can be seen in the diagram above, the use of the shared BMS would actually be transparent for the ECRIS community and in particular for the ECRIS Central Authorities. The national ECRIS TCN system would still act as a technical interface to the central ECRIS TCN system, which would expose the set of required services.
- The ECRIS TCN solution is based on the assumption that fingerprints are collected in controlled environments, are of very good quality and are packaged in the form of NIST files (which is an international standard supported by all AFIS products). Considering the fact that the requirements for the ECRIS TCN solution on quality and availability of fingerprints are higher than in other large-scale EU systems to date, it can be reasonably assumed that the target levels of quality and formats of the fingerprints to be collected and stored for ECRIS TCN will be sufficient for the integration with the shared BMS. In other words, this study assumes that the integration with the shared BMS would not significantly change the collection and processing of fingerprints in the context of ECRIS TCN, compared to the solution relying on a dedicated central AFIS.
- The requirements for the centralised ECRIS TCN solution in terms of system availability and response times are significantly lower than what is required for other large-scale EU systems used for border control or management of VISA applications. It can reasonably be assumed that the shared BMS will be designed right from the start for meeting higher technical requirements than what is needed for ECRIS TCN (i.e. designed for a high availability set-up, most probably already supporting clustering, load-balancing, replication of servers and data, etc.).

Figure 16 Centralised ECRIS TCN solution: architecture with integration with the shared BMS



5.2.1 Cost assessment: use of a shared BMS

Cost estimates cannot be established as detailed information enabling the quantification of costs of using a shared BMS in the centralised ECRIS TCN solution was not available at the moment this study was conducted. The remainder of this section provides a qualitative assessment on the potential cost impact of integrating the centralised ECRIS TCN solution with the shared BMS.

Following various meetings with eu-LISA, AFIS vendors, European Commission representatives and ECRIS technical experts, conducted in the beginning of 2017, the study provides the following indications:

- This study assumes that the shared BMS will in principle not be oversized when going live. This means that for the extra storage capacity and processing power required for ECRIS TCN, additional resources will need to be purchased and set-up at the level of the shared BMS, specifically to cover the needs of the central ECRIS TCN system.
- According to the information received from vendors, the main factors determining the cost of an AFIS are the number of fingerprint records expected to be stored, the number of processing operations to be handled per day and the response times that are expected for matching operations (especially if very fast responses are required under high load). This impacts directly

the cost of the hardware to be purchased for the installation of the AFIS but also the cost of the software license for the product itself.

- For the reasons mentioned above, additional expenses must be expected for the purchase and set-up of dedicated hardware as well as the increased license costs for the central AFIS in the shared BMS. This could result only in marginal cost savings compared to the costs to be expected for purchasing and setting up a dedicated AFIS in the central ECRIS TCN system.
- Some cost savings could be expected from the use of the shared BMS on parts that are shared between all connected systems and that do not require specific additional resources. This mainly concerns parts of the underlying physical infrastructure (database servers, network, virtualisation servers, firewalls, etc.) and services, in particular maintenance and support activities.
- The cost savings mentioned above could be partially or even completely counterbalanced by the additional effort and the increased complexity brought by the technical integration between the central ECRIS TCN system and the shared BMS itself. It can be reasonably assumed that a dedicated AFIS would be tailored specifically to the needs of the central ECRIS TCN system and would be easier to integrate from a technical point of view.
- No cost savings are expected from the customisation and tuning of the AFIS parameters. Indeed, a system integrated with the shared BMS has specific needs in terms of matching algorithms, fingerprint quality thresholds and accuracy levels. This implies that additional work needs to be done for the analysis of these parameters and the customisation of the AFIS included in the shared BMS needs to be done also for the ECRIS TCN solution.
- In terms of timing, in case a shared BMS is implemented it is likely that it will be designed and implemented in parallel to the design and implementation of the ECRIS TCN solution. From this situation two possibilities emerge:
    - The shared BMS will be operational before the centralised ECRIS TCN solution: in this case the centralised ECRIS TCN solution can be adapted during its design phase, so as to directly foresee the integration with the shared BMS rather than setting up a dedicated AFIS as a subsystem of the central ECRIS TCN system. At the same time, the design of the shared BMS can take into account the needs of the centralised ECRIS TCN system. This scenario should not have significant additional impacts on the costs of the solutions.
    - The centralised ECRIS TCN solution will be operational before the shared BMS: in this case it is necessary in a first phase to foresee the procurement and set-up of a dedicated AFIS as a subsystem of the central ECRIS TCN system. In a second phase, once the shared BMS is operational, a technical migration must be envisaged to replace the dedicated central AFIS by an integration with the shared BMS. This scenario has a significant impact on costs as it requires the procurement and set-up of a dedicated AFIS which is then replaced by the shared BMS for which also additional equipment and licenses need to be purchased and set-up. In addition extra effort needs to be foreseen for analysing and implementing the migration from the dedicated

AFIS to the shared BMS. At this point, the fingerprints already stored in the dedicated AFIS will also need to be transferred to the common AFIS so as to ensure the continuity of ECRIS TCN. The cost of the AFIS is not doubled in this scenario because the hardware purchased for the dedicated AFIS can probably be reused to some extent for increasing the capacity of the shared BMS.

Overall, regarding costs, no significant savings should be expected from the integration with a shared BMS. In the worst case it could even lead to additional costs when compared to the use of a dedicated AFIS in the central ECRIS TCN system.

The main advantage of using the shared BMS would be to provide possibilities of cross-referencing and verifications across multiple systems, which would possibly increase the level of internal security in the EU as well as the quality of identification for the purposes of ECRIS TCN. The following two examples illustrate these advantages:

1. Fingerprints of a TCN convicted in a Member State are uploaded through the central ECRIS TCN system in the shared BMS. At the insertion into the shared BMS, the system detects that the fingerprints match with the ones provided in an existing SIS II[65] alert entered by another Member State. This scenario would allow the competent authorities that have issued the alert – in this case police forces – to be informed that the TCN being searched has actually been convicted in another Member State, possibly under another nominal identity. These police forces would then be able to contact the convicting Member State and to take the necessary actions in accordance with the SIS alert.
2. The ECRIS Central Authorit**y in a Member State triggers a** 'hit/no hit' search in the central ECRIS TCN system so as to determine which other Member State(s) possibly have conviction information on the given TCN subject. The central ECRIS TCN system internally performs a search in its alphanumeric search engine and a *one-to-many* search in the shared BMS. It could very well be the case that no hits are found in the identity records provided by other ECRIS Central Authorities although the TCN subject was convicted in the past under another name because fingerprints were not captured at that moment with the conviction. If the *one-to-many* search in the shared BMS was also performed on fingerprints uploaded through other sources, for example through VIS (Visa Information System) or SIS II (Schengen Information System Second Generation), it could possibly result in 'hits' revealing that the same individual has used other identities not known in the judicial world in the past. The requesting ECRIS Central Authority could then be informed of such alternate nominal identities and widen the scope of the initial 'hit/no hit' search.

Currently the specific EU systems have been established based on specific European and national legislation that strictly regulates their usage and defines which competent authorities are authorised to manipulate the information. Integrating ECRIS TCN with the shared BMS would require this legislation

[65] SIS II stands for Schengen Information System Second Generation)

to be adapted in order to further regulate the extended usage of the identification information, including fingerprints that would be uploaded into the shared BMS. In particular, the rights and obligations of each of the involved competent authorities would need to be revised for the cases of cross-referencing and cross-matching. Also, it can be expected that hits in any of the systems would need to be followed up by information exchanges between the involved competent authorities. This additional exchange of information between different authorities in different Member States would also need to be regulated.

5.3 Direct access by third parties

Direct access to central EU security and border control databases for Europol and Eurojust has become the norm over the past years, and further extensions to this direct access are being considered at the moment by the European Commission. The reasons for granting such direct access are easily understood – both Europol and Eurojust have legitimate reasons for accessing the information in these systems, as this completes their view on certain criminal phenomena, and can be used directly for preventing and combating crime.

The question therefore needs to be answered whether such direct access to the central ECRIS TCN system by Europol and Eurojust would also be warranted. Similarly, national law enforcement authorities and judicial authorities within Member States could also possibly benefit from direct access to the central ECRIS TCN system. This is a political choice to be made by the EU legislators.

However, functional and operational limitations as described in section 5.1.1, also apply in this case; the central ECRIS TCN system does not contain any information on convictions and a hit would only inform that the given person has 'possibly' been convicted in the indicated Member State(s). Therefore, subsequent information exchanges would be necessary between the third party (i.e. Europol, Eurojust, etc.) and the concerned ECRIS Central Authorities. It must be noted that the base ECRIS principle is that each Central Authority acts as a single point of contact for obtaining information on criminal records when the data exchanges take place between different EU Member States. In practice, in each Member State, the national authority managing the central national criminal records register is also the one acting as ECRIS Central Authority. Therefore, even if third parties would be able to access the central ECRIS TCN system, it would be necessary to ensure that in the case of hits the third party could contact the national criminal records authorities for further information. Existing information channels between these third parties and national authorities could be used for this.

Providing direct access to third parties to the central ECRIS TCN system will also mean regulating technical and administrative issues, in particular around managing access rights, providing the tools to access the system to authorities, providing additional training and monitoring the usage made by third parties, etc. Finally, such direct access would need to be authorised and regulated through appropriate European and national legislation.

At this stage, only a limited number of third parties could benefit from such direct access (Europol, Eurojust, and the European Public Prosecutors Office). It is also unclear how many searches would be issued by them.

5.3.1 Cost assessment: direct access by third parties

At this stage, it is not possible to provide cost estimates for the impact of giving direct access to third parties with the centralised ECRIS TCN solution. The main obstacle for estimating these cost impacts is the lack of detailed information on how many third parties would benefit from direct access to the centralised ECRIS TCN solution and, more importantly, how many searches would be issued by them. Therefore multiple assumptions would need to be made, making the cost estimation calculation not reliable at this point in time.

6 Extensions of the centralised ECRIS TCN solution

This section assesses the feasibility, advantages, disadvantages and cost impact of possible extensions of the centralised ECRIS TCN solution. The extensions of ECRIS TCN features and scope assessed in this study are a result of interactions between the European Commission and Member States. In this study we assess the extension of the centralised ECRIS TCN solution to:

- Include EU nationals in the central ECRIS TCN system, as presented in section 6.1;
- Include one-to-one matching of fingerprints, as presented in section 6.2
- Include browsing, viewing and retrieving features, as presented in section 6.3; and
- Include the use of facial images as an additional biometric identifier, as presented in section 6.4.

6.1 Inclusion of EU nationals in the central ECRIS TCN system

As described in section 1, ECRIS currently works well for EU nationals but is inadequate for TCN, which is why a solution based on a central system and including fingerprints has been elaborated. This solution will be designed not only to enable exchanges between EU Member States relating to a TCN, but also to maximise efficiency and the accuracy of the system as much as possible. It would thus be reasonable to also evaluate the possibility of expanding the centralisation of data to include the identity information of convicted EU nationals in view of further increasing the efficiency of ECRIS.

6.1.1 Scenario

If the identity records of convicted EU nationals are centralised, then the current ECRIS principles and information exchanges, which are based on the Member State of nationality acting as a point of reference, also need to be revised. Several possibilities can be imagined. For the sake of this study, the following scenario is assumed:

- The Member State of nationality no longer acts as reference point. The identities of all convicted persons (i.e. EU nationals, EU non-nationals[66] and TCN) are uploaded by the convicting Member States and are kept in the central ECRIS TCN system.
- The concept of notification, used to inform the Member State of nationality that one of its nationals has been convicted in another Member State, is replaced by an upload into the central ECRIS TCN system of the identity of the convicted person and of the Member State holding the conviction information. The process becomes identical to the upload of identity records of convicted TCN.
- When a Member State needs to find information on past convictions for an EU citizen, its ECRIS CA needs to first query the central ECRIS TCN system to identify which other Member State(s) possibly hold such information. This also applies for the own Member State's nationals, as they

[66] In this study the term EU non-national is used to refer to nationals of an EU Member State other than the convicting Member State.

might have been convicted in the past in another Member State. This process becomes identical to the query for information on past convictions for TCN (i.e. which is done in practice by using the national ECRIS TCN system for querying the central ECRIS TCN system, and subsequently sending ECRIS requests to all other Member States for which 'hits' have been returned).

6.1.2 Impacts and qualitative assessment

The following benefits can be expected from the extension:

- There would no longer be the need to notify the convictions of EU nationals to the Member State of nationality. Such notifications currently amount to around 40 000 per month, or around 25% of the total transactions performed through ECRIS. These notifications, which convey the whole information on the convictions of EU non-nationals to their respective Member States of nationality, are replaced by a much simpler registration in the central ECRIS TCN system of the identity of the convicted person (without any details on offences, sanctions, additional decision, etc.). Currently each convicting Member State must also keep the Member State of nationality informed about subsequent changes being applied to convictions of the EU non-nationals. This is also no longer necessary. Only changes to the convicted persons' identity records need to be communicated to the central ECRIS TCN system (which is a lot less frequent), as well as their removal when the conviction's retention period has been reached. This approach could thus simplify and reduce the administrative burden associated, especially for Member States that record and send the notification messages manually in their ECRIS system.[67]
- In the current ECRIS, fingerprints exchanges are only rarely used. Less than a third of the EU Member States rely on fingerprints for the identification of persons on a systematic or regular basis. The centralisation of fingerprints and their systematic use at central level for automatic identification based on biometrics, could increase the reliability of the identification of the EU national concerned. Of course, this would depend on the willingness of Member States to include fingerprints in the ECRIS central database, and a positive assessment of the proportionality of doing so.
- Centralising the identity information and fingerprints of EU nationals would also mean that there would not be a difference in the treatment of the information and efficiency levels of ECRIS between EU nationals, EU non-nationals and TCN. From a practical and administrative point of view this simplifies the work because persons involved in the daily operations in the Central Authorities can adopt the same (or similar) internal procedures independently of the nationality of the person for which a query has been issued.

This approach would have the following drawbacks:

- European and national legislation would need to be adapted in order to regulate the centralisation and use of identification information, including the fingerprints of EU nationals.

[67] Discussion note ECRIS-TCN and ECRIS – issues related to the establishment of a central database supporting the ECRIS Expert Group Meeting 10-11 January 2017, DG JUST

- Adding the identity information of EU nationals to the central ECRIS TCN system leads to an increase in the volume of data that needs to be stored and processed at a central level, leading to higher costs of setting up the solution presented in section 6.1.3.
- Since Member States would no longer receive conviction information from other countries, they would need to query the central ECRIS TCN system in all cases, even for their own nationals, whereas in the current system they have the conviction information on their own nationals immediately available. It counterbalances the advantage stated above (i.e. notifications no longer being sent through ECRIS) by an increase in the number of ECRIS requests sent between Member States. This may lead to an additional administrative burden for the ECRIS CA. In addition, it may also increase the time needed for the national criminal records authority to provide an answer in the case of a query for a national for which 'hits' have been found in other Member States, since ECRIS requests need to be sent to these other Member States.
- The fact that the Member State of nationality would no longer centralise the conviction information of its own nationals implies changes in the operational procedures currently carried out by the Central Authorities, but also changes in the distribution of the administrative burdens across Member States. Currently a Member State with a high percentage of its nationals residing abroad will receive a proportionate amount of notifications and requests to process in ECRIS, independent of how many convictions are handed down at national level. By implementing this option, the administrative burden shifts and becomes proportionate to the number of convictions handed down at national level rather than to the number of nationals living abroad.

This extension of the central ECRIS TCN system would have the following technical impacts:

- The detailed technical specifications of ECRIS and the existing ECRIS systems (including the ECRIS Reference Implementation software provided by Commission) need to be modified as follows:
    - Notifications are removed;
    - Currently a request sent to an EU Member State by definition concerns either a national of that country or a TCN. This needs to be expanded so that any Member State can receive and respond to requests concerning persons of any nationality (i.e. nationals, EU non-national and TCN).
- Following the changes brought to the detailed technical specifications of ECRIS and to the ECRIS Reference Implementation, Member States need to adapt their national systems accordingly while implementing or integrating with ECRIS. In particular, Member States that have already automated the drafting and sending of notifications to other Member States in ECRIS would need to revise this automation and send the identity records of the convicted persons to the central ECRIS TCN system instead.
- Additional capacity needs to be foreseen for the central ECRIS TCN system to cope with the increase in number of identity records and increase in number of processing operations.

6.1.3 Cost assessment: inclusion of EU nationals in the centralised ECRIS TCN solution

This section provides the description, assumptions and estimations of the incremental costs related to the extension of the central ECRIS TCN system by including EU nationals. As explained in section 6.1, this scope extension would require:

- Update of the ECRIS technical specifications and update of the ECRIS Reference Implementation: the costs for these updates are accounted as part of the implementation of the centralised ECRIS TCN solutions as presented in section 4.2.
- Update of the ECRIS implementation at national level following the updates of the ECRIS technical specifications: the cost for this update cannot be calculated at this stage given the lack of details on the possible operation of the centralised ECRIS TCN solution including EU nationals.
- Upgrade of the central AFIS system component and the central alphanumeric search engine: the inclusion of EU nationals' identity data and fingerprints in the central ECRIS TCN system would require an upgrade of the central AFIS system component and the central alphanumeric search engine. The incremental costs of these subsystems vary according to the number of identity records to be stored in the central ECRIS TCN system and the number of processing operations to be handled per day.
- Backlog: for the purpose of this study it is assumed that, by the entry into force of the ECRIS TCN legislation, the Member States will have registered approximately 75,8 million alphanumeric identity records and 25 million fingerprints of convicted persons in total (including EU nationals, EU non-nationals and TCN). Although the volumes are significantly higher than for TCN only, it is assumed that the technical components used for loading the alphanumeric identity records and fingerprints into the central ECRIS TCN system are designed in such a way that they can handle this increase without the need to change the infrastructure or design of these components. Essentially the estimated effort for building these technical components is expected to be the same, but more legacy data will need to be uploaded.

Therefore the incremental costs of extending the central ECRIS TCN system by including EU nationals of additional hardware, software, development and maintenance costs for the central AFIS system component and the central alphanumeric search engine.

Table 5 below presents the incremental costs incurred by the European Union to include EU nationals in the central ECRIS TCN system as detailed in section 3 and Table 11 presents the incremental costs for including EU nationals in the interoperable, highly available ECRIS TCN system, as detailed in section 5.1. The cost estimates take into account the volumes of data and number of processing operations to be handled by the national and central ECRIS TCN systems as presented in Annex II.

Table 9 Extension: Inclusion of EU nationals to the central ECRIS TCN system

Costs incurred by the European Union (*in million EUR, to three decimal places)*	Incremental one-off costs (3 years)	Incremental ongoing costs (1 year)
Central ECRIS TCN system Upgrade of the central AFIS system component • Description: This extension includes the functionality of making convicted EU nationals searchable via the ECRIS TCN solution. This implies that identity data of all convicted EU nationals are included in the central ECRIS TCN system. This extension includes additional hardware, software, development and maintenance costs for the central AFIS system component. • Assumptions: It is assumed that the use of this extension should handle the following system requirements: o Database size including records from TCN and EU nationals (67 million records, 3 300 new records per hour, 3 900 one-to-many searches per hour); o Availability: 97% uptime, 5 days per week, during working hours;	7,365	1,180
Central ECRIS TCN system Upgrade of the central alphanumeric search engine • Description: This extension includes the functionality of making convicted EU nationals searchable via the ECRIS TCN solution. This implies that identity data of all convicted EU nationals are included in the central ECRIS TCN system. This extension includes additional software, development and maintenance costs for the central alphanumeric search engine. • Assumptions: It is assumed that the use of this extension should handle the following system requirements: o Database size including records from TCN and EU nationals (117,8 million records, 3 300 new records per hour, 3 900 1:n searches per hour); o Availability: 97% uptime, 5 days per week, during working hours;	2,970	0,180
Total costs: European Union	10,335	1,360

Source: WAVESTONE Data Analysis, April 2017.

As shown in Table 9, the total incremental one-off costs incurred by the European Union to extend the central ECRIS TCN system to include EU nationals are approximately EUR 10 million over a time period of three years of system implementation and the total incremental ongoing costs are approximately EUR 1,4 million per operating year.

Table 10 Extension: Inclusion of EU nationals in the highly available central ECRIS TCN system

Costs incurred by the European Union (*in million EUR, to three decimal places)*	Incremental one-off costs (3 years)	Incremental ongoing costs (1 year)
Highly available central ECRIS TCN system Upgrade of the highly available central AFIS system component • Description: This extension includes the functionality of making convicted EU nationals searchable via the ECRIS TCN solution. This implies that identity data of all convicted EU nationals are included in the central ECRIS TCN system. This extension includes additional hardware, software, development and maintenance costs for the highly available central AFIS system component. • Assumptions: It is assumed that the use of this extension should handle the following system requirements: o Database size including records from TCN and EU nationals (67 million records, 3 300 new records per hour, 3 900 1:n searches per hour); o Highly available system (99.99%, 24/7 during 365 days per year);	10,535	2,335
Highly available central ECRIS TCN system Upgrade of the highly available central alphanumeric search engine • Description: This extension includes the functionality of making convicted EU nationals searchable via the ECRIS TCN solution. This implies that identity data of all convicted EU nationals are included in the central ECRIS TCN system. This extension includes additional software, development and maintenance costs for the highly available central alphanumeric search engine. • Assumptions: It is assumed that the use of this extension should handle the following system requirements: o Database size including records from TCN and EU nationals (117,8 million records, 3 300 new records per hour, 3 900 one-to-many searches per hour); o Highly available system (99.99%, 24/7 during 365 days per year);	4,455	0,297
Total costs: European Union	14,990	2,632

Source: WAVESTONE Data Analysis, April 2017.

As shown in Table 10, the total incremental one-off costs incurred by the European Union by extending the highly available central ECRIS TCN system to include EU nationals, are approximately EUR 15 million over a time period of three years of system implementation, and the total incremental ongoing costs are approximately EUR 2,6 million per operating year.

6.2 One-to-one matching of fingerprints

Following the study conducted in 2016[68], Member States have largely expressed their preference for a centralised solution for ECRIS TCN. The main reason for this preference was the significantly lower cost and lower complexity of including fingerprints in the ECRIS TCN exchanges using a centralised solution. During the discussions and further analysis of the centralised scenarios that were presented, several Member States indicated that if a central ECRIS TCN system is put in place, then it could also provide additional features that would help their Central Authority respond to ECRIS requests concerning TCN, which is done at national level.

As described in the ECRIS TCN processes presented in section 3.2, the initial 'hit/no hit' search does not aim to identify the TCN but rather at determining which other Member State(s) can be queried for

[68] Final Report, Feasibility study on the inclusion of pseudonymised fingerprints in ECRIS TCN exchanges, Kurt Salmon, Intrasoft, GLSI, Brussels, 30 June 2016.

information on past convictions. Then the ECRIS requests are sent by the requesting CA to those Member States that were found during the 'hit/no hit' search. When replying to an ECRIS request, it is the responsibility of the requested CA to search the relevant information and to gain a sufficient level of confidence that the past conviction data found indeed corresponds to the person for which the request was issued. The search of past conviction data is performed differently in each Member State depending on the available sets of information and tools used at national level by the CA.

Member States highlighted that it would be useful if the requested CA could perform additional verifications using the central ECRIS TCN system for cases where fingerprints are provided in the ECRIS request. In case multiple individuals match the identity information provided in the ECRIS request and the CA can retrieve their fingerprints at national level, the CA could run *one-to-one* matching using the central ECRIS TCN system to verify identities. *One-to-one* matching could also be used for confirming the initial 'hit' received by the requesting CA (e.g. useful for cases where the *one-to-one* matching uses different, more accurate algorithms than the *one-to-many* matching).

The main benefit of extending the centralised ECRIS TCN solution to include *one-to-one* matching of fingerprints is that the solution would provide an additional tool that can help the Member States' CA in responding better to ECRIS requests. This would increase the quality, reliability and efficiency of the identification of the TCN. Nevertheless, the benefits of this extension are limited given that the *one-to-many* matching done earlier by the requesting Member State is already expected to be accurate enough to minimise false-positive hits. In the majority of cases, the fingerprints triggering a hit with *the one-to-many* matching will also trigger a hit when compared directly with the *one-to-one* matching algorithm.

The main technical impacts of this extension relate to the upgrade of the central AFIS system component, specifically:

- Additional hardware capacity needs to be foreseen for the AFIS embedded in the central ECRIS TCN system for handling the extra load brought by the *one-to-one* matching operations, executed in addition to the regular uploads of identity records and one-to-many searches.
- Depending on the vendor providing the AFIS that is embedded in the central ECRIS TCN system, additional license costs are to be expected. Depending on the specific AFIS solution chosen, it could require a separate installation and/or different sets of algorithms.
- Additional analysis, development, testing, maintenance and support effort needs to be foreseen for implementing this extension for both national and central ECRIS TCN systems.

The number of such *one-to-one* matching operations is not known at the time of writing. For the purpose of estimating costs, it is assumed that this extension would roughly represent 30% of the 'hit/no hit' searches. This means that the central ECRIS TCN system would then need to be able to handle a load of 138 *one-to-one* searches per hour (1 100 per day) in addition to the already foreseen processing operations for storing TCN identity records and for responding to one-to-many searches.

6.2.1 Cost assessment: one-to-one matching using fingerprints

This section provides the description, assumptions and estimations of the incremental costs related to the extension of the central ECRIS TCN system by including the *one-to-one* matching of fingerprints. As explained in section 6.2, this extension would require the upgrade of the central AFIS system component with additional hardware, software, development, and maintenance costs. The incremental costs of the upgrading the central AFIS system component vary according to the number of identity records that need to be stored, the number of processing operations to be handled per day and the response times that are expected for matching operations.

This study assesses the incremental cost of including *one-to-one* matching of fingerprints in the following cases:

- *One-to-one* matching of fingerprints extending a centralised ECRIS TCN solution, including only TCN fingerprints;
- *One-to-one* matching of fingerprints extending a highly available centralised ECRIS TCN solution, including only TCN fingerprints;
- *One-to-one* matching of fingerprints extending a centralised ECRIS TCN solution, including fingerprints of TCN and EU nationals; and
- *One-to-one* matching of fingerprints extending a highly available centralised ECRIS TCN solution, including fingerprints of TCN and EU nationals.

Table 11 below presents the incremental costs incurred by the European Union to include *one-to-one* matching of fingerprints in the four cases presented above.

Table 11 also details the assumptions taken in each of the aforementioned cases.

The possible incremental cost impacts of adapting national systems to perform *one-to-one* matching using the central ECRIS-TCN system were not assessed in this study given several possibilities and a lack of details on the possible operation of this extension at national level.

Table 11 Extension: One-to-one matching using fingerprints

Costs incurred by the European Union (*in million EUR, to three decimal places)*	Incremental one-off costs (3 years)	Incremental ongoing costs (1 year)
Central ECRIS TCN system Biometric verification – One-to-One matching • Description: This extension includes an additional feature enabling Member States to perform one-to-one matching using the central ECRIS TCN system. • Assumptions: It is assumed that the use of this extension should handle the following system requirements: o Database size including records from TCN only (14 million records, 400 new records per hour, 460 one-to-many searches per hour); o Availability: 97% uptime, 5 days per week, during working hours; o Maximum additional one-to-one searches: 138 per hour.	0,417	0,050

Costs incurred by the European Union (*in million EUR, to three decimal places)*	Incremental one-off costs (3 years)	Incremental ongoing costs (1 year)
Highly available central ECRIS TCN system Biometric verification – One-to-One matching • Description: This extension includes an additional feature enabling Member States to perform one-to-one matching using the highly available central ECRIS TCN system. • Assumptions: It is assumed that the use of this extension should handle the following system requirements: o Database size including records from TCN only (14 million records, 400 new records per hour, 460 one-to-many searches per hour); o Highly available system (99,99%, 24/7 during 365 days per year); o Maximum additional one-to-one searches: 138 per hour.	0,472	0,095
Central ECRIS TCN system including EU nationals Biometric verification – One-to-One matching • Description: This extension includes an additional feature enabling Member States to perform one-to-one matching using the central ECRIS TCN system. • Assumptions: It is assumed that the use of this extension should handle the following system requirements: o Database size including records from TCN and EU nationals (67 million records, 3 300 new records per hour, 3 900 1:n searches per hour); o Availability: 97% uptime, 5 days per week, during working hours; o Maximum additional one-to-one searches: 1 200 per hour.	0,435	0,060
Highly available ECRIS TCN system including EU nationals Biometric verification – One-to-One matching • Description: This extension includes an additional feature enabling Member States to perform one-to-one matching using the highly available central ECRIS TCN system. • Assumptions: It is assumed that the use of this extension should handle the following system requirements: o Database size including records from TCN and EU nationals (67 million records, 3 300 new records per hour, 3 900 one-to-many searches per hour); o Highly available system (99,99%, 24/7 during 365 days per year); o Maximum additional one-to-one searches: 1 200 per hour.	0,513	0,100

Source: WAVESTONE Data Analysis, April 2017.

According to the cost assessment, the incremental costs for the *one-to-one* matching functionally do not vary a lot depending on the database size or availability requirements. It can be concluded that the worst case scenario in terms of costs (i.e. *one-to-one* matching of fingerprints extending a centralised ECRIS TCN solution with high availability including fingerprints of TCN and EU nationals) would be to add a *one-to-one* matching functionality using fingerprints to the central ECRIS TCN system, adding approximately EUR 0,5 million in incremental one-off costs over three years of system implementation, and EUR 0,1 million in incremental yearly ongoing costs.

6.3 Browsing, viewing and retrieving features

In the proposed centralised ECRIS TCN solution, described in section 3, Member States will upload identity records (i.e. alphanumeric identity information and fingerprints) of TCN convicted at national level into the central ECRIS TCN system. Each CA retains the full ownership of the identity records that it has uploaded in the central system.

For this reason, Member States have expressed that they would like to be able to access their own TCN identity records in the central ECRIS TCN system. In particular, each CA would need to have the possibility to browse, search, view and retrieve their TCN identity records.

The main benefits of extending the centralised ECRIS TCN solution to allow browsing, viewing and retrieving of identity records would be the following:

- The additional features would facilitate the daily operational usage of the ECRIS TCN systems and would support trouble-shooting activities (i.e. analysis and investigation done by the CA at national level, in case the ECRIS exchanges yield unexpected or unwanted results).
- An indirect benefit would be that CA would not need to keep fingerprints at the level of the national criminal records register, but only a unique technical reference. They could directly benefit from the storage provided by the central ECRIS TCN system.

The technical impact of extending the centralised ECRIS TCN solution to provide browsing, viewing and retrieving features for identity records is mainly the increased effort for additional analysis, development, testing and maintenance for implementing and operating these functions in both the national and the central ECRIS TCN systems. Such features are usually provided out-of-the-box by the AFIS products. The work would therefore consist in making these features accessible at the central ECRIS TCN system (through remote technical services such as web services) and in the graphical user interface of the national ECRIS TCN systems deployed in Member States.

6.3.1 Cost assessment: browsing, viewing and retrieving features

As explained in section 6.3, these features are provided out-of-the-box by the AFIS products such as the one foreseen to be implemented as the central AFIS system component. This means that this extension would not imply incremental costs regarding hardware and software licences. However, it is expected that incremental costs would incur regarding the necessary additional effort for analysis, development, testing and maintenance effort for implementing and operating these functionalities in both the national and the central ECRIS TCN systems.

At this stage, it is not possible to estimate the incremental costs of extending the centralised ECRIS TCN solution enabling browsing, viewing and retrieving features. The main obstacle for estimating the incremental cost of this extension is the lack of information on how the functionalities and related business process would work in the context of the centralised ECRIS TCN solution. Therefore, multiple assumptions would need to be made making the cost estimation calculation not reliable at this point in time.

6.4 Use of facial images as additional biometric identifier

During the discussions in the Council Working Party over the past year on the initial Commission's proposal of January 2016[69], a broad consensus on using fingerprints to assist in the identification of convicted TCN has emerged. However, other large-scale European systems use other biometric identifiers in addition to fingerprints for identifying persons. For example, the Entry Exit System (EES)[70] system which was proposed by the Commission in April 2016 also refers to facial images as a biometric identifier to be used. The Schengen Information System Second Generation (SIS II)[71] should in the future allow for the use of palm prints, facial images and DNA profiles. The Prüm arrangements[72] also foresee the possibility to compare DNA profiles. The European Commission has thus requested to also explore the possibility to include facial images as an additional biometric identifier in the centralised ECRIS TCN solution.

Since a few years there has been a general trend to try to combine as much as possible several biometric identifiers in order to enhance the accuracy of biometric searching and matching. Foreseeing the inclusion of facial images in the centralised ECRIS TCN solution would make the system future-proof. This study however does not go as far as also evaluating the inclusion of other biometric identifiers such as DNA or iris scans, which would require separate studies on their own.

Moreover, facial images are included in the scope of this study also because they are expected to be a possible 'quick win' as such images could be easily captured – along with the fingerprints – without excessive additional complexity and costs to Member States. The eu-LISA Smart Borders technical pilot[73] demonstrated that live facial image enrolment can be accomplished by either using a standard off-the-shelf web camera in good environmental conditions or by extracting from a picture, an RFID e-document which is compliant with ICAO standard 9303[74]. Facial images can thus indeed be taken with low-cost material, such as high-definition webcams or electronic RFID reader, which have become over the years standard, cheap off-the-shelf products that are easy to operate.

In addition, visual comparison of facial images could already be done at national level by human operators, without need for specific expertise or expensive matching systems, and would provide an additional tool for facilitating the identification of a TCN. Finally, facial recognition algorithms could also possibly be included in the central ECRIS TCN system, at the level of the central AFIS component and combined with the alphanumeric and fingerprint matching algorithms, in order to further increase the accuracy of the 'hit/no hit' search. The main drawbacks of this option are the following:

[69] Proposal for a Directive of The European Parliament and of The Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, 19 January, Brussels.

[70] Stronger and Smarter Borders in the EU: Commission proposes to establish an Entry-Exit System, European Commission press release, Brussels, 6 April 2016.

[71] Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II).

[72] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

[73] Smart Borders Pilot Project, Report on the technical conclusions of the Pilot, Volume 1, eu-LISA, supported by PWC, 2015.

[74] ICAO standard 9303 is an international standard for machine readable travel documents, including electronic EU passports.

- The implementation of the ECRIS TCN solution requires further changes in European and national legislation so as to allow capturing, storing and using fingerprints as biometric identifiers for TCN. Additional changes in European and national legislation would need to be foreseen in order to also regulate the capturing, storing and usage of facial images in the context of ECRIS TCN.
- Capturing facial images will require additional organisational changes and equipment at the national level; this is however balanced out by the fact that the facial images could be captured at the same stage as the fingerprints, with minor additional complexity, and that the costs expected for acquiring and setting up high-definition webcams is very low compared to the overall cost of implementing ECRIS TCN.

The scope of this study is limited to evaluating the impacts of capturing, uploading and storing facial images of convicted TCN so as to enable their retrieval and visual comparison by human operators. Therefore, the use of facial recognition software and combining facial recognition algorithms with the fingerprint matching algorithms has not been further assessed in this study.

The main technical impact of extending the centralised ECRIS TCN solution to provide functions for uploading, storing and retrieving facial images is the increased effort for additional analysis, development, testing and the maintenance needed to implement these functions in both the national and the central ECRIS TCN systems. Additional hardware is also necessary for storing the facial images in the central ECRIS TCN system but this is negligible considering that storing 1 million facial images requires approximately 20 GB of hard drive space (in case of facial images for TCN only, this would amount to a total space of 100 GB; in case of facial images for EU nationals and TCN it would amount to a total space of 1 TB).

6.4.1 Cost assessment: use of facial images in the centralised ECRIS TCN solution

This section provides the description, assumptions and estimations of the incremental costs related to the extension of the centralised ECRIS TCN solution by including the storage of facial images as additional biometric identifiers. As explained in section 6.4, this extension would require the increase of storage capacity and additional analysis, development, testing and maintenance to implement the facial images storage extension.

The incremental costs of this extension have thus been estimated on the basis that facial images would be captured by Member States and uploaded into the centralised ECRIS TCN solution for storage. Facial images would then be sent back to the requesting or requested Member State in case of a hit, to facilitate visual verification done by human operators in the ECRIS Central Authorities.

From a technical point of view it is also assumed that:

- The facial images used follow the ICA standard 9303 (same technical standard and format used for the electronic EU passports);
- The size for data storage is of 20kB per facial image (this translates into a maximum of 20 GB for 1 million facial images).

Based on these assumptions, the volume of storage needed for the facial images of convicted TCN is estimated at 100 GB while an additional 1 TB would be needed in case EU nationals are added to the scope of the centralised ECRIS TCN solution (details in section 6.1). Based on the data collected, the cost of storage in a system such as the centralised ECRIS TCN solution is considered negligible. Therefore the incremental cost of this extension is mainly related to the additional analysis, development, testing and maintenance to implement the facial images storage extension in the national and central ECRIS TCN system.

Table 12 below presents the incremental costs for extending the central ECRIS TCN system by including the storage of facial images as additional biometric identifier. The incremental costs of extending the national ECRIS TCN systems including the storage of facial images are not accounted in this study given the lack of information available on the possible different implementations of this extension at national level.

Table 12 Extension: Use of facial images as additional biometric identifiers

Costs incurred by the European Union (*in million EUR, to three decimal places)*	One-off costs (3 years)	Ongoing costs (1 year)
Facial images as additional biometric identifier • Description: This extension allows Member States to upload and store facial images of convicted TCN to the central ECRIS TCN system and to use them as additional biometric identifiers. This cost item accounts the additional development and maintenance costs to extend the centralised ECRIS TCN solution to provide functions for uploading, storing and retrieving facial images. • Assumptions: It is assumed that the additional hardware costs to implement this functionality are negligible given the estimated size of the database (up to 1 Tb) and its availability requirements.	0,207	0,041

Source: WAVESTONE Data Analysis, April 2017.

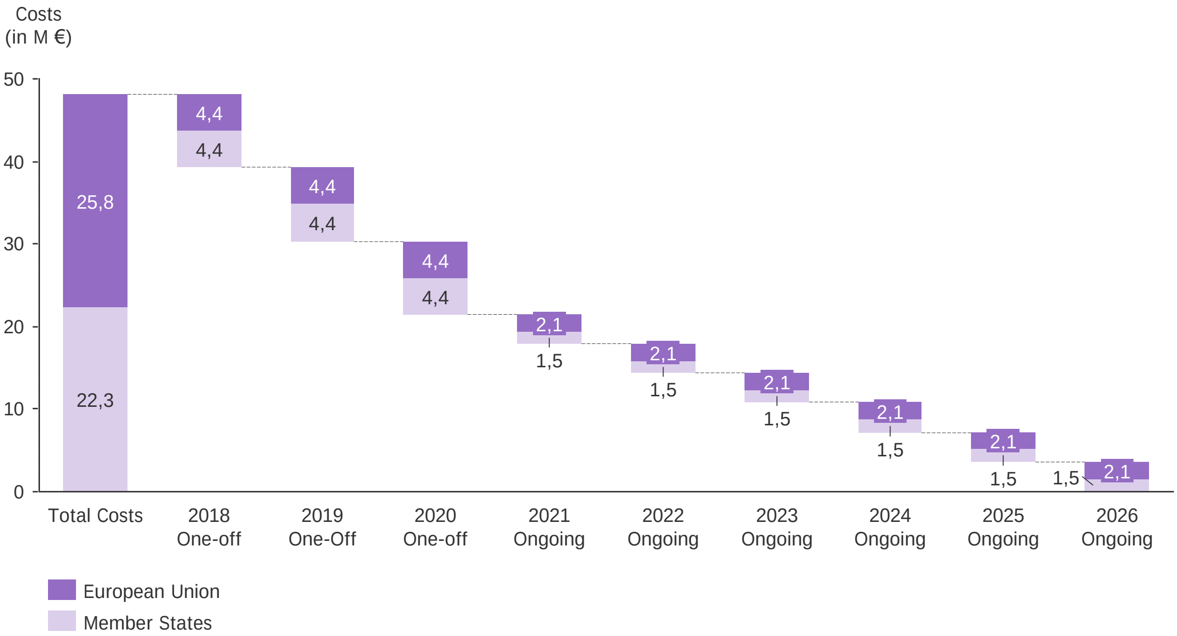
As shown in Table 8, the total incremental one-off costs incurred by the European Union to extend the central ECRIS TCN system by including the storage of facial images as an additional biometric identifier are approximately EUR 0,2 million over a time period of three years of system implementation and the total incremental ongoing costs are approximately EUR 0,04 million per operating year.

7 Conclusions

This section presents the conclusions on the feasibility and cost assessment of the establishment of a centralised ECRIS TCN solution as well as the impacts of ensuring the interoperability, future-proofing, and extensions of the foreseen system.

This study detailed the high level architecture, key principles and processes of the envisaged centralised ECRIS TCN solution. The proposed centralised ECRIS TCN solution addresses the current two main challenges of ECRIS: (i) the inefficiency in the ECRIS exchanges regarding TCN, by enabling 'hit/no hit' searches identifying the Member State(s) holding previous convictions of a TCN and (ii) the issues on the identification of the specific convicted person by including fingerprints as identifier of a convicted person. Technically, the solution focuses on fulfilling the current requirements of ECRIS, specifically with regard to availability, response time and storage capacity. In this context the cost impact of implementing a centralised ECRIS TCN solution is approximately EUR 48 million, EUR 26 million incurred by the European Union and EUR 22 million incurred by the Member States. Figure 17 below shows the breakdown of the incurred costs over three years of implementation (i.e. one-off costs) and the first six years of system operations (i.e. ongoing costs). Other views on the cost impacts of the implementation of the centralised ECRIS TCN solution are presented in section 4.2.

Figure 17 Centralised ECRIS TCN solution: Total costs summary



Source: WAVESTONE Data Analysis, March 2017.

This study also investigated the feasibility and cost impacts of ensuring the interoperability, future-proofing, and extensions of the foreseen system. These are important aspects to be considered in the decision making process of the European Commission which would address needs beyond the ones currently highlighted by the ECRIS community. These aspects would enable the use of ECRIS by a broader audience and extend its initial scope and features.

The integration of the centralised ECRIS TCN solution with other European large scale systems would facilitate the access of data on convicted persons to other stakeholders beyond the justice domain (e.g. migration, home affairs, border control, etc.).

While this integration is technically feasible, it entails functional, operational and legal impacts, given that data exchanges between the centralised ECRIS TCN solution and any other large scale system impact need to be clearly identified and regulated by European and national legislations. This would also add administrative burdens on the ECRIS Central Authorities that would need to provide responses to new requesting authorities and for different purposes than those foreseen by the current ECRIS. Technically, the integration of the central ECRIS TCN system with large scale systems such as the ones used in the immigration and border control domains (e.g. SIS II, ETIAS, EES) would require that the central ECRIS TCN system complies with significantly higher requirements on availability (99.99% instead of 97%) and target response time (real-time instead of up to one hour). This study estimated that a highly available central ECRIS TCN system would costs approximately EUR 15 million more than a central ECRIS TCN system for a nine-year period; accounting EUR 6,6 million one-off costs for the system implementation and EUR 1,4 million yearly ongoing costs for the system operation. This additional cost is mostly related to the need to update the IT infrastructure, the central component for monitoring and analytics, the central AFIS system component and the central alphanumeric search engine to comply with the high availability requirements.

This study also investigated the possibility of using a shared Biometric Matching Services (BMS) for the central ECRIS TCN system rather than setting up a dedicated central AFIS component. Similar to the integration with other EU large scale systems, integrating the centralised ECRIS TCN solution with a shared BMS would require national and EU legislation to be adapted in order to further regulate the extended usage of the identification information, including fingerprints that would have been uploaded into the shared BMS. At the time this study was performed, DG HOME and eu-LISA were still studying the impacts, technical feasibility and possible scenarios for the establishment of a shared BMS. Nevertheless, this study drew the preliminary conclusion that it is technically feasible to use a shared BMS in the envisaged centralised ECRIS TCN solution. At this point in time, it can be reasonably assumed that the functions needed by the central ECRIS TCN system (i.e. storage of fingerprints and *one-to-many* matching) will be covered out-of-the-box by the shared BMS as these are basic features provided by all commercial AFIS products. The impacts of using the shared BMS would be that a different architecture would be put in place, although the key principles and characteristics of the centralised ECRIS TCN solution would remain identical. Regarding costs, even if the quantification of costs is not possible at this point in time, based on the qualitative data collected in this study, no significant savings would result from the integration of the centralised ECRIS TCN solution in a shared BMS. In the worst case it could even lead to additional costs when compared to the use of a dedicated AFIS in the central ECRIS TCN system.

In line with the investigation of enabling the use of ECRIS TCN by a broader audience, this study investigated the possibility of granting direct access to ECRIS TCN to third parties such as Eurojust and Europol. Providing such access to third parties would imply functional, operational and legal considerations. Similar to the impacts of integrating the ECRIS TCN solution with other EU systems, this access would need to be authorised and regulated through appropriate European and national legislation and would lead to an increased number of requests to be handled by ECRIS central authorities. Moreover, providing direct access to third parties to the centralised ECRIS TCN solution would also require technical and administrative changes, in particular: managing access rights; providing authorities with access tools to the system; providing additional training and monitoring the usage made by third parties. At this stage, it is not possible to provide cost estimates for the impact of providing direct access to third parties with the centralised ECRIS TCN solution. The main obstacle for estimating these cost impacts is the lack of detailed information on how many parties would benefit from direct accesses to the centralised ECRIS TCN solution and how many searches would be issued by them.

The functionalities enabled by a centralised ECRIS TCN solution could also increase the efficiency of ECRIS regarding EU nationals. In this context the study investigated the impacts of extending the ECRIS TCN solution by including the identity data of convicted EU nationals. This extension would eliminate the need to notify convictions of EU nationals to the Member State of nationality, therefore reducing administrative burdens. Centralising the identity information and fingerprints of EU nationals would also mean that there would not be a difference in the treatment of the information and in the level of efficiency of ECRIS between EU nationals and TCN. Nevertheless, this extension would require changes in European and national legislation as well as drastic changes in ECRIS business processes, as the Member State of nationality would no longer centralise the conviction information of its own nationals. At the technical level, adding the identity information of EU nationals to the central ECRIS TCN system leads to an increase in the volume of data that needs to be stored and processed at a central level, increasing the set up and operational costs of the central ECRIS TCN system. The incremental costs are mainly related to the upgrade of the central AFIS system component and the central alphanumeric search engine. This study estimated that including EU nationals in the ECRIS TCN system would increase the cost of the centralised ECRIS TCN solution by approximately EUR 18,5 million for a nine-year period; accounting EUR 10 million one-off costs for the system implementation and EUR 1,4 million yearly ongoing costs for the system operation. The costs are higher for a highly available central ECRIS TCN system, increasing the cost by approximately EUR 30,8 million for a nine-year period; accounting for EUR 15 million in one-off costs for the system implementation and EUR 2,6 million in yearly ongoing costs for the system operation.

Another extension to the centralised ECRIS TCN investigated in this study is the inclusion of *one-to-one* matching of fingerprints. The inclusion of this feature would enable CA's to perform additional verifications using the central ECRIS TCN system for cases where fingerprints are provided in the ECRIS request. This would help the Member States' CA by increasing the quality, reliability and efficiency of the identification of the TCN. Nevertheless, the benefits of this extension are limited given that the *one-to-many* matching done earlier by the requesting Member State is already expected to be accurate enough so as to minimise false-positive hits. The main technical impacts of this extension relate to the upgrade of the central AFIS system component. This would impact incremental costs as follows:

- *One-to-one* matching of fingerprints extending a centralised ECRIS TCN solution including only TCN fingerprints: approximately EUR 0,7 million for a nine-year period; accounting for EUR 0,4 million in one-off costs for the system implementation and EUR 0,05 million yearly ongoing costs for the system operation.
- *One-to-one* matching of fingerprints extending a highly available centralised ECRIS TCN including only TCN fingerprints: approximately EUR 1 million for a nine-year period; accounting for EUR 0,4 million in one-off costs for the system implementation and EUR 0,1 million in yearly ongoing costs for the system operation.
- *One-to-one* matching of fingerprints extending a centralised ECRIS TCN solution including fingerprints of TCN and EU nationals; approximately EUR 0,7 for a nine-year period; accounting for EUR 0,4 million in one-off costs for the system implementation and EUR 0,06 million in yearly ongoing costs for the system operation.
- *One-to-one* matching of fingerprints extending a highly available centralised ECRIS TCN solution including fingerprints of TCN and EU nationals: approximately EUR 1 million for a nine-year period; accounting for EUR 0,5 million in one-off costs for the system implementation and EUR 0,1 million in yearly ongoing costs for the system operation.

Member States have also expressed that they would like the central ECRIS TCN system to enable them to access the identity records of TCN convicted by their Member State. This would allow each CA to have the possibility to browse, search, view and retrieve their TCN identity records. The extension of the centralised ECRIS TCN solution to allow browsing, viewing and retrieving features of identity records would facilitate the daily operational usage of the ECRIS TCN systems by the CA. As such features are usually provided out-of-the-box by the AFIS product, the technical impact of this extension would need additional analysis, development, testing and maintenance efforts to implement and operate these functions in the national and the central ECRIS TCN systems. At this stage, it is not possible to estimate the incremental costs of extending the centralised ECRIS TCN solution enabling browsing, viewing and retrieving features. The main obstacle for estimating the incremental cost of this extension is the lack of information on how the functionalities and related business process would work in the context of the centralised ECRIS TCN solution.

Finally this study also evaluated the impacts of extending the centralised ECRIS TCN solution to include facial images as an additional biometric identifier. The scope of this study is limited to evaluating the impacts of capturing, uploading and storing facial images of convicted TCN so as to enable their retrieval and visual comparison by a human operator. The use of facial recognition software and the combination of facial recognition algorithms with fingerprint matching algorithms has not been assessed by this study. The main technical impact of extending the centralised ECRIS TCN solution to provide for these functions would be additional efforts in analysis, development, testing and maintenance, needed to implement these functions in both the national and the central ECRIS TCN systems. Even if additional hardware is necessary for storing the facial images in the central ECRIS TCN system, the cost impact of this storage would be negligible (e.g. facial images for TCN would amount to a total space of 100 GB; facial images for both EU nationals and TCN it would amount to a total space of 1 TB). This study estimated that extending the centralised ECRIS TCN solution to include facial images as an additional biometric identifier would increase the cost of the centralised ECRIS TCN solution by approximately EUR 0,5 million over a nine-year period; accounting for EUR 0,2 million in one-off costs for the system implementation and EUR 0,04 million in yearly ongoing costs for the system operation.

Table 13 below summaries the incremental cost impacts of the assessed extensions of the centralised ECRIS TCN solution.

Table 13 Summary of incremental costs for extensions of the centralised ECRIS TCN solution

Extensions of the centralised ECRIS TCN solution (*in million EUR, to three decimal places)*	Incremental one-off costs (3 years)	Incremental ongoing costs (1 year)
Highly available central ECRIS TCN system	6,567	1,439
Use of a shared Biometric Matching Service	Costs not available	Costs not available
Direct access by third parties	Costs not available	Costs not available
Including EU nationals to the central ECRIS TCN system	10,335	1,360
Including EU nationals to the highly available central ECRIS TCN system	14,990	2,632
Central ECRIS TCN system, Biometric verification – One-to-One matching	0,417	0,050
Highly available central ECRIS TCN system, Biometric verification – One-to-One matching	0,472	0,095
Central ECRIS TCN system including EU nationals, Biometric verification – One-to-One matching	0,435	0,060
Highly available ECRIS TCN system including EU nationals, Biometric verification – One-to-One matching	0,513	0,100
Browsing, viewing, and retrieving own identity records	Costs not available	Costs not available
Facial images as additional biometric identifiers	0,206	0,041

Annex I. Detailed Methodology

This section presents in detail the steps of the ISA Method[75] used to conduct the Feasibility study and cost assessment of the establishment of a centralised ECRIS TCN solution.

Step I: Define the scope of the ICT Assessment

The first step of the methodology is to define the scope of the ICT Assessment of the legislative proposal for a centralised ECRIS TCN solution as described in section 3.

For this purpose, the following actions were performed:

- Identification of the ICT relevance of the policy problem and objectives;
- Identification of the stakeholders affected by the technical solution; and
- Definition of the technical solution.

i) Identify the ICT relevance of the policy problem and objectives

The first step of the ICT Assessment methodology is to identify the ICT relevance of the policy problem and the objectives of the study. In this study, this step is performed by assessing the challenges that ECRIS currently faces and the feasibility of the establishment of a centralised ECRIS TCN solution. This is presented in detail in section 1.

ii) Analyse stakeholders

A stakeholder analysis was performed in order to identify all groups of individuals impacted by the proposed technical solution.

> Stakeholder analysis provides means to identify the relevant stakeholders who have a 'stake' or interest in the study under consideration.

Table 14 provides a summary of the different stakeholder groups affected by the technical solution defined in section 3.

[75] The ISA Method for Assessing ICT Implications of EU Legislations is applied to the assessment of cost impacts, 2015.

Table 14 Summary of the stakeholder groups

Stakeholder Group code (SG)	Stakeholder Group Name (SGN)	Size of the stakeholder group	Description of the stakeholder group
SG01	European Union	• DG JUST • eu-LISA	• The European Commission – operates the common communication infrastructure and assists Member States in preparing the technical infrastructure for interconnecting their criminal records databases by adopting a number of technical measures. This group includes officials from DG JUST. This group will be affected by the assessed technical solution. The European Commission will be involved in the overall governance and coordination of the ECRIS TCN project. Detailed mapping of each cost item affecting the European Commission stakeholder group is presented in the following sections. • eu-LISA[76] - European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice. This stakeholder group will be affected by the assessed technical solution. Eu-LISA will be responsible for the overall development, maintenance and support of the centralised ECRIS TCN solution.
SG02	The ECRIS Central Authority (CA)	28 ECRIS Member State Central Authorities	• CA – This group includes the competent authorities from the 28 EU Member States representing 28 ECRIS Member State Central Authorities which store criminal record data in national databases and exchange them electronically upon request. ECRIS Central Authorities will be affected by the implementation of the centralised ECRIS TCN solution.

iii) Define the technical solution

Several technical solutions and variants for the implementation of an ECRIS TCN exchanges with the inclusion of fingerprints have been identified. The technical solutions were narrowed down to eight possible technical solutions which were described and assessed in the ECRIS TCN cost assessment study conducted in 2016[77]. The study indicated that a centralised solution would be the favourite option for the purposes of ECRIS TCN exchanges. Furthermore, following the June 2016 Justice and Home Affairs Council, where a large majority of Member States had indicated support for implementing a centralised solution for ECRIS TCN, the Commission has had another look in detail at the technical, legal and policy issues which follow from this preference. Therefore, this study thoroughly assesses the technical feasibility and cost impact for implementing a centralised ECRIS TCN solution. The detailed description of the assessed technical solution is presented in section 3.

Additionally, inspired by the Commission's communication 'Stronger and Smarter Information Systems for Borders and Security'[78] and requested by the European Commission, this study also assesses the technical feasibility and when possible the cost impact of making the centralised ECRIS TCN solution interoperable and future-proofed as presented in section 5, as well as possible extensions presented in section 6.

[76] European Agency for the operational management of large-scale IT systems in the area of freedom security and justice.

[77] Final Report, Feasibility study on the inclusion of pseudonymised fingerprints in ECRIS TCN exchanges, Kurt Salmon, Intrasoft, GLSI, Brussels, 30 June 2016.

[78] Communication from the Commission to the European Parliament and the Council, Stronger and Smarter Information Systems for Borders and Security, COM(2016) 205 final, Brussels, 6.4.2016.

Step II: Prepare the ICT Cost Assessment

The second step of the methodology aimed to prepare the ICT Assessment. For this purpose, two key actions, detailed in the following sections, were performed:

- Building the ICT cost model for the technical solution; and
- Defining the data collection methods to be applied.

i) Build the ICT cost model

The Better Regulation Guidelines[79] and Better Regulation Toolbox[80] set a list of criteria that will allow comparisons of the ICT based technical solution to be assessed in a full Impact Assessment study. Within the scope of the current study, the ICT Assessment is focused on two main criteria: cost efficiency and technical feasibility of the proposed technical solution.

Based on the Better Regulation Toolbox, the cost efficiency criterion is defined as substantive compliance costs.

> Substantive compliance costs encompass the incremental (i.e. non-business as usual) costs to the target group of complying with regulation other than fees and administrative costs.

This study assesses substantive compliance costs (incremental costs) according to the ICT cost categories specified in the Better Regulation Toolbox as follows:

- Hardware costs – provide the total (anticipated) cost of the hardware (e.g. network, servers) required to develop, support, operate and maintain the system. Hardware costs are accounted as one-off costs (i.e. investment costs related to the establishment of the system) and as ongoing costs (i.e. recurring cost for the maintenance of the hardware, including replacement of the hardware).
- Software costs – provide the total (anticipated) cost of software (e.g. applications, libraries) required to develop, support, operate and maintain the system. Software costs are accounted as one-off costs (i.e. investment costs related to the establishment of the system) and as ongoing costs (i.e. recurring cost for the maintenance of the software, including upgrades).
- Development costs – provide the total (anticipated) cost (human resources and other) for the development of the system (e.g. analysis and process reengineering activity, coding activity, project management activity, test activity, configuration & change management activity, deployment activity). Development costs are accounted as one-off costs (i.e. investment costs related to the establishment of the system).
- Maintenance costs – provide the total (anticipated) cost (human resources and other) in person days per year to maintain the system (e.g. activities related to both corrective

[79] Better Regulation Guidelines [COM (2015)205 final] European Commission, 19.05.2015.
[80] Better Regulation Toolbox #23 ICT Assessment, The Digital Economy and Society SWD(2015) 111 final, European Commission, 19.5.2015.

maintenance and evolving maintenance). Maintenance costs are accounted as ongoing costs (i.e. incremental recurring costs of operation of the system).

- Support costs – provide the total (anticipated) cost (human resources) in person days per year to support the system (e.g. helpdesk, operations). Support costs are accounted as ongoing costs (i.e. incremental recurring costs of operation of the system).

The first step to build a cost model is breaking down the technical solution into cost items for which costs can be assessed with an adequate level of detail. Secondly, each cost item is associated with one or more of the abovementioned categories of ICT costs by taking into account whether these costs are one-off or ongoing. Thirdly, the costs incurred for the implementation of each cost item are calculated as a sum of cost categories associated to it. And finally, the total cost of the technical solution is defined by the sum of each of its cost items.

Table 15 presents the technical solution decomposed into cost items and the associated cost categories. The table also shows whether one-off and ongoing costs are associated to each cost item and cost category. Maintenance and support costs are associated to recurring costs (i.e. yearly recurring costs). Infrastructure and development activities are associated to one-off costs. An exception to that is the recurring infrastructure costs associated to the cost item ‘IT infrastructure of the central ECRIS TCN system (97% availability). This recurring infrastructure costs are related to the hardware and software yearly fees incurred by eu-LISA to operate their technical infrastructure. Each cost item is explained in detail in section 4.

Table 15 Centralised ECRIS TCN solution: Cost items and ICT cost categories

Cost Category Cost Items	Hardware		Software		Development		Maintenance		Support	
	One-off	Ongoing	One-off	Ongoing	One-off	Ongoing	One-off	Ongoing	One-off	Ongoing
1 - IT infrastructure of the central ECRIS TCN system	☑	☑	☑	☑	☑			☑		☑
2 - Central component for loading alphanumeric identity records and fingerprints					☑			☑		☑
3 - Central alphanumeric search engine			☑		☑			☑		☑
4 - Central AFIS system component	☑		☑		☑			☑		☑
5 -Central component for monitoring and analytics					☑			☑		☑
6 - Technical specification for the ECRIS TCN solution					☑					
7 - Update of the ECRIS technical specifications					☑					
8 - Update the ECRIS Reference Implementation					☑					
9 - Development of Reference Implementation for the national ECRIS TCN system					☑			☑		☑
10 - ECRIS TCN management					☑			☑		☑
11 - IT infrastructure of the national ECRIS TCN system	☑		☑		☑			☑		☑
12 - National component for extracting and transmitting alphanumeric identity records and fingerprints					☑			☑		
13 - Setup of the national ECRIS TCN system					☑			☑		☑
14 - Update of national AFIS for verification following a hit in the central ECRIS TCN system			☑		☑					

Table 16 below presents the list of the assessed extensions of the centralised ECRIS TCN solution.

Table 16 Extensions of the centralised ECRIS TCN solution

Cost Category Cost Items	Hardware		Software		Development		Maintenance		Support	
	One-off	Ongoing	One-off	Ongoing	One-off	Ongoing	One-off	Ongoing	One-off	Ongoing
IT infrastructure of the highly available central ECRIS TCN system	☑	☑	☑	☑	☑					☑
Central component for monitoring and analytics (highly available)					☑			☑		
Highly available central AFIS system component	☑				☑			☑		☑
Highly available central alphanumeric search engine			☑		☑			☑		☑
Central ECRIS TCN system: Biometric verification – One-to-one matching	☑		☑		☑			☑		
Highly available central ECRIS TCN system: Biometric verification – One-to-one matching	☑		☑		☑			☑		
Central ECRIS TCN system including EU nationals: Biometric verification – One-to-one matching	☑		☑		☑			☑		
Highly available ECRIS TCN system including EU nationals: Biometric verification – One-to-one matching	☑		☑		☑			☑		
Including EU nationals – Upgrade of the central AFIS system component	☑		☑		☑			☑		
Including EU nationals – Upgrade of central alphanumeric search engine			☑		☑			☑		
Including EU nationals – Upgrade of highly available central AFIS system component	☑		☑		☑			☑		
Including EU nationals – Upgrade of highly available central alphanumeric search engine			☑		☑			☑		
Facial images as additional biometric identifiers					☑			☑		

ii) Define the data collection methods

Based on the stakeholder analysis' results and on the specifications of this study, desk research, cost assessment questionnaires, interviews and benchmarking with similar technical solutions, were the data collection methods considered as the most appropriate for conducting this study.

The Desk Research is the instrument to screen and collect legal, policy, and technical information from documentation available at EU level and therefore to be able to assess the current situation of the exchange of criminal records information on convicted TCN and the use of fingerprints in the 28 Member

States and EU systems. Additionally, to ensure the effective and efficient collection of data, the project team emphasised the need to systematically conduct appropriate ex-ante desk research, in order to better frame the scope of the study, prior to using any other data collection method (e.g. interviews). The data collection covered legal texts, studies regarding similar EU systems, policy documentation, expert group meeting summary reports and additional documents related to the current situation on the use of fingerprints technologies within the scope of the study.

As a direct input, this study is using data collected in the scope of two cost assessments conducted consequently in 2015[81] and 2016[82].

In 2015, an online questionnaire was elaborated and sent out to the National Competent Authorities from the 28 Member States representing ECRIS's Member State Central Authorities and an interview was conducted with eu-LISA. The cooperation with eu-LISA continued throughout 2016. A dedicated questionnaire targeting specifically the centralised ECRIS TCN solution was elaborated and sent out to eu-LISA in February 2017. A set of interviews and meetings were conducted in March 2017 in order to validate and clarify the input provided by eu-LISA.

In the scope of the 2016 study, primary data was collected during a workshop with AFIS vendors, held on 15 March 2016, in Brussels. The workshop focused on the technical aspects of one-to-many matching of pseudonymised fingerprints in the context of ECRIS TCN. Primary data was also collected through interviews conducted with AFIS[83] vendors. All interviews were supported by a structured questionnaire with a set of questions. Follow-up interviews with AFIS vendors were performed in 2017.

For data protection and business confidentiality purposes, the individual answers received from vendors, ECRIS experts, eu-LISA and the Member States are treated anonymously, remained confidential, were only disclosed to the evaluation team and were used solely for research purposes.

Finally, all collected data was extrapolated and used for the analysis of the technical scenarios presented in this study. The detailed list of data sources and calculation of estimates is presented in Annex III.

Step III: Assess the ICT impacts

The third and last phase of the methodology aimed to assess the ICT impacts by performing the following activities:

- Collect and analyse data; and
- Comparison of the technical solutions.

i) Collect and analyse data

[81] Information Communication Technology (ICT) Final Report, Assessment of ICT impacts of the legislative proposal for ECRIS TCN system regarding the exchange of convictions for third country nationals and stateless people (TCN), Kurt Salmon, Brussels, 4 December 2015.

[82] Final Report, Feasibility study on the inclusion of pseudonymised fingerprints in ECRIS TCN exchanges, Kurt Salmon, Intrasoft, GLSI, Brussels, 30 June 2016.

[83] Private enterprises specialised in security and identity solutions with experience in biometric matching technologies.

This study is based primarily on desk research activities, on data collected from the CA stakeholder group and on cost estimates provided by eu-LISA, as well as data provided by vendors. In order to control the quality of the collected data, the Project Team used the RACER (Relevant, Accepted, Credible, Easy to monitor and Robust against manipulation) technique, as mentioned in the Better Regulation toolbox[84]: The RACER technique is composed of the following elements:

- Relevant: closely linked to the objectives to be reached (in this case, measured). Relevance indicators should not be overambitious and should measure the right thing (e.g. a target indicator for health care could be used to reduce waiting times but without jeopardising the quality of care provided).
- Accepted: The role and responsibilities for the indicator need to be well defined (e.g. if the indicator is the handling time for a grant application and the administrative process is partly controlled by Member States and partly by the EU, then both sides would assume only partial responsibility).
- Credible: Indicators should be simple and robust, unambiguous and easy to interpret. If necessary, composite indicators might need to be used instead – such as country ratings, well-being indicators, but also ratings of financial institutions and instruments. These often consist of aggregated data using predetermined fixed weighting values. As they may be difficult to interpret, they should be used to assess broad contexts only.
- Easy to monitor (e.g. data collection should be possible at low cost).
- Robust against manipulation: e.g. if the target is to reduce administrative burdens to businesses, the burdens might not be reduced, but just shifted from businesses to public administration.

The data analysis of the technical solution is presented in section 4.

ii) Comparison of the technical solutions

The assessment of the technical solution is presented in detail in section 4. Based on this assessment, conclusions were drawn and presented in section 7. This study assesses the cost impacts of establishing a centralised ECRIS TCN solution, therefore no comparison of technical solutions is presented.

[84] Better Regulation Toolbox #35 Monitoring arrangements and indicators, complementing SWD(2015) 111 final, Commission Staff Working Document, Better Regulation Guidelines, {COM(2015) 215 final} {SWD(2015) 110 final}, Strasbourg, 19.5.2015.

Annex II. ECRIS TCN Volumetric information

The volumes of data and number of processing operations to be handled by the national and central ECRIS TCN systems are key elements for estimating their cost impact. This section details the volumes that have been estimated for the national and central ECRIS TCN systems.

The volumetric information presented in this study is calculated based on the data provided by the Member States in 2014. A series of assumptions are made with regard the number of convictions of TCN and of EU nationals, and based on current ECRIS trends and figures. Several numbers are rounded up or maximised to have a slightly more cautious approach, accounting for worst case situations.

- In average 700 000 convictions against TCN are handed down throughout the EU per year. To simulate a peak year in the calculations of number of processing operations, 10% is added to this number (i.e. 770 000 per year).
- In average 6 million convictions are handed down in total throughout the EU per year (including EU nationals and TCN). To simulate a peak year in the calculations of number of processing operations, 10% is added to this number (i.e. 6,6 million per year).
- For all convictions, fingerprints are captured and uploaded into the central ECRIS TCN system, irrespectively of the type and severity of the offence. This is most certainly not representative of the real implementation of the ECRIS TCN solution. However, no other more realistic figures can be extrapolated at this stage of the study and therefore the worst possible situation is taken as assumption for calculating the estimations.
- The central authorities of Member States in the EU operate 250 days per year.
- NIST files provided as input to the central ECRIS TCN system contain ten-print images with a high level of quality. The NIST files stored within the central AFIS contain the fingerprint images, with small amount of text data, and a compression rate set around 12:1. The average size of such a file is 1,5 MB. An additional 0,4 MB is added per NIST file for the storage within the AFIS of the fingerprint template (i.e. binary representation of the fingerprint minutiae, used for indexation and search of the fingerprints).
- To estimate the amount of ECRIS requests concerning TCN subjects, it is assumed that the same trends as for EU nationals apply. The ECRIS numbers of requests and notifications exchanged between November 2015 and May 2016 in the EU have been used to extrapolate yearly amounts. This results in the following base numbers:
    - Estimated average amount of ECRIS requests: 346,000 per year;
    - Estimated average amount of new convictions notified through ECRIS: 291,000 per year;
    - On a yearly basis, there are 19% more requests than new notifications;
    - Approximately 77% of ECRIS requests are issued for criminal proceedings, 23% are for purposes other than criminal proceedings.

- It is assumed that all Member States perform the backlog (i.e. upload of all available legacy data) at the go-live of the ECRIS TCN solution. By the entry into force of the ECRIS TCN legislation, the Member States will have registered:
  - for convicted TCN: approximately 9,1 million alphanumeric identity records and 3 million fingerprints;
  - for all convicted persons (EU nationals and TCN included): approximately 75,8 million alphanumeric identity records and 25 million fingerprints.

Volumetric for the national ECRIS TCN system – TCN only

The volumes of data to store and number of operations to process for the national ECRIS TCN system directly depends on how many convictions the Member State is handing down at national level against TCN. This determines how many new identity records are uploaded in the national ECRIS TCN system but also determines how many requests relating to TCN are sent, and thus how many 'hit/no hit' search queries need to be performed. This statement is reinforced by the fact that 77% of ECRIS requests are issued for criminal proceedings, the majority thus occurring during the pre-trial stages.

For this purpose, the Member States have been categorised in the following levels:

- High: Member States handing down in average between 90 000 and 270 000 convictions against TCN per year (using a maximum of 297 000 convictions for peak years);
- Medium: Member States handing down in average between 10 000 and 90 000 convictions against TCN per year (using a maximum of 99 000 convictions for peak years);
- Low: Member States handing down in average less than 10 000 convictions against TCN per year (using a maximum of 11 000 convictions for peak years).

Table 17 and Table 18 below detail the volumetric information used as basis for estimating the capacity of the national ECRIS TCN system, depending on the levels defined above:

Table 17 National ECRIS TCN system: maximum number of processing operations

Number of processing operations (peaks)	max/daily	max/yearly
LOW level		
Number of identity records uploaded at national level	45	11 000
Number of 'hit/no hit' queries to trigger	55	13 000
MEDIUM level		
Number of identity records uploaded at national level	400	100 000
Number of 'hit/no hit' queries to trigger	475	118 000
HIGH level		
Number of identity records uploaded at national level	1 200	297 000
Number of 'hit/no hit' queries to trigger	1 450	354 000

Table 18 National ECRIS TCN system: maximum number of identity records and storage capacity

Number of identity records and storage (cumulated, after 7 years of operations)	
LOW level	
Number of alphanumeric identity records	210 000
Number of NIST files	120 000
Disk space required for fingerprints (raw NIST files)	180 GB
MEDIUM level	
Number of alphanumeric identity records	2 million
Number of NIST files	1,1 million
Disk space required for fingerprints (raw NIST files)	1,6 TB
HIGH level	
Number of alphanumeric identity records	3,9 million
Number of NIST files	2,5 million
Disk space required for fingerprints (raw NIST files)	3,8 TB

The maximum numbers of processing operations and maximum number of identity records are taken as basis for estimating the target capacity, and thus the cost relating to the national ECRIS TCN system. They both correspond to the 'high' level category.

Volumetric for the central ECRIS TCN system – TCN only

The following volumetric information is used as basis for estimating the costs of the central ECRIS TCN system and of its subsystems (i.e. the alphanumeric search engine and the central AFIS):

Table 19 Central ECRIS TCN system: maximum number of processing operations

Number of processing operations (peaks)	max/daily	max/yearly
Number of identity records uploaded from all EU Member States (max in peak year)	3 100	770 000
Number of hit/no hit queries to process	3 700	916 000

Table 20 Central ECRIS TCN system: maximum number of identity records and storage capacity

Number of identity records and storage (cumulated, after 7 years of operations)	
Number of alphanumeric identity records	14 million
Number of NIST files	7,9 million
Disk space required for fingerprints (raw NIST files and fingerprint templates)	15 TB

Volumetric for the national ECRIS TCN system – TCN and EU nationals

The volumes of data and number of processing operations to be handled by the centralised ECRIS TCN solution and its subsystems increase significantly in case the scope is extended by including EU nationals. The distribution across the EU of convictions being different compared to the solution including only TCN, the Member States have been categorised across the following levels:

- High: Member States handing down in average between 500 000 and 1,4 million convictions per year (using a maximum of 1,54 million convictions for peak years);
- Medium: Member States handing down in average between 100 000 and 500 000 convictions per year (using a maximum of 550 000 convictions for peak years);
- Low: Member States convicting in average less than 100 000 convictions per year (using a maximum of 110 000 convictions for peak years).

Table 21 and Table 22 show the expected data volumes to be processed by the national ECRIS TCN systems if the scope of the centralised ECRIS TCN solution is extended to include EU nationals.

The maximum numbers of processing operations and maximum number of identity records are taken as basis for estimating the target capacity for the national ECRIS TCN system. They both correspond to the 'high' level category.

Table 21 National ECRIS TCN system: number of processing operations including EU nationals

Number of processing operations (peaks)	max/daily	max/yearly
LOW level		
Number of identity records uploaded at national level	440	110 000
Number of hit/no hit queries to trigger	525	131 000
MEDIUM level		
Number of identity records uploaded at national level	2 200	550 000
Number of hit/no hit queries to trigger	2 650	655 000
HIGH level		
Number of identity records uploaded at national level	6 200	1,6 million
Number of hit/no hit queries to trigger	7 350	1,8 million

Table 22 National ECRIS TCN system: number of identity records and storage capacity including EU nationals

Number of identity records and storage (cumulated after 7 years of operations)	
LOW level	
Number of alphanumeric identity records	2,1 million
Number of NIST files	1,2 million
Disk space required for fingerprints (raw NIST files)	1,8 TB
MEDIUM level	
Number of alphanumeric identity records	11 million
Number of NIST files	6 million
Disk space required for fingerprints (raw NIST files)	9 TB
HIGH level	
Number of alphanumeric identity records	21,3 million
Number of NIST files	13,6 million
Disk space required for fingerprints (raw NIST files)	21 TB

Volumetric for the central ECRIS TCN system – TCN and EU nationals

Table 23 and Table 24 show the expected data volumes to be processed by the central ECRIS TCN system if the scope of the centralised ECRIS TCN solution is extended to include EU nationals.

Table 23 Central ECRIS TCN system: number of processing operations including EU nationals

Number of processing operations (peaks)	max/daily	max/yearly
Number of identity records uploaded from all EU Member States (max in peak year)	26 400	6,6 million
Number of hit/no hit queries to process	31 400	7,9 million

Table 24 Central ECRIS TCN system: number of identity records and storage capacity including EU nationals

Number of identity records and storage (cumulated, after 7 years of operations)	
Number of alphanumeric identity records	118 million
Number of NIST files	67 million
Disk space required for fingerprints (raw NIST files and fingerprint templates)	128 TB

Variations on volumetric calculations and impacts on cost estimates

This study assumes that the ECRIS TCN solution will be ready in 2020 and calculates operational costs until 2026. It must be noted that if the solution is ready one year later or one year earlier, it impacts only slightly the estimated target capacity of the ECRIS TCN systems. The estimated number of processing operations is calculated based on the throughput expected per year, and is thus not affected at all by the date of the go-live of the ECRIS TCN solution. As a result, a shift of one year in the calendar for the implementation of the ECRIS TCN systems would not impact noticeably the related one-off cost.

As an example, the tables below show the resulting number of identity records of TCN to store in the central ECRIS TCN system when the go-live is shifted by one year:

Table 25 Central ECRIS TCN system: maximum number of identity records and storage capacity (go-live in 2019)

Number of identity records and storage (go-live in 2019, cumulated, after 7 years of operations)	
Number of alphanumeric identity records	13,5 million
Number of NIST files	7,8 million
Disk space required for fingerprints (raw NIST files and fingerprint templates)	15 TB

Table 26 Central ECRIS TCN system: maximum number of identity records and storage capacity (go-live in 2021)

Number of identity records and storage (go-live in 2021, cumulated, after 7 years of operations)	
Number of alphanumeric identity records	14,5 million
Number of NIST files	8,1 million
Disk space required for fingerprints (raw NIST files and fingerprint templates)	15,5 TB

As shown in the tables above, the target capacity of the central ECRIS TCN system only varies little when shifting the calendar of implementation of the ECRIS TCN solution by one year. Considering the fact that this would only impact the costs relating to the initial set-up of the AFIS and of the alphanumeric search engine that are included in the central ECRIS TCN system, it can be safely concluded that this has a negligible impact on the overall one-off costs (approximately +/- 40 000 EUR)[85].

[85] The incremental cost indicated here has been estimated using linear interpolation, calculated on the basis of the cost estimates used for the scenario including EU nationals. The result of this interpolation provides a cost variation of 12 500 EUR per 100 000 fingerprint records and 14 300 EUR per 500 000 alphanumeric identity records.

Annex III. Data sources and calculation of estimates

This section details the calculation of each cost item composing the analysed technical scenarios including the main data sources and the calculation approach used to estimate the costs of each cost item.

Table 27 Data sources and data extrapolation techniques

Incurred by	Cost item	Data source	Data extrapolation
European Union	IT infrastructure of the central ECRIS TCN system	• eu-LISA • Data extrapolation technique	• Cost estimates are based on data provided by eu-LISA. The data has been thoroughly analysed and adapted to the specific ECRIS TCN system requirements. • Hardware costs account for all components of the central ECRIS TCN system with the exception of the central AFIS. • Maintenance costs are accounted under cost item 10 ECRIS TCN management. • Support costs account for 0.5 FTE (daily fee 500 EUR over 240 days) equivalent to 60 000 EUR yearly support cost.
European Union	Central component for loading alphanumeric identity records and fingerprints	• eu-LISA • Data extrapolation technique	• Cost estimates are based on data provided by eu-LISA. The data has been thoroughly analysed and adapted to the specific ECRIS TCN system requirements.
European Union	Central alphanumeric search engine	• Alphanumeric search engine vendor	• Cost estimates provided by specialised vendor. No data extrapolation technique applied.
European Union	Central AFIS system component	• AFIS Vendors • Data extrapolation technique	• Cost estimates are based on data provided by specialised vendors. • Average cost value calculated using 'Simple Average' i.e. average value of data collected.
European Union	Central component for monitoring and analytics	• eu-LISA	• Cost estimates provided by eu-LISA. No data extrapolation technique applied.
European Union	Technical specification for the ECRIS TCN solution	• ECRIS technical specialist	• Cost estimates provided by ECRIS technical specialist. No data extrapolation technique applied. • Financial calculations done on the following basis: o Effort is estimated in person-days; o The cost estimates are based on the usage of senior persons (e.g. project manager, senior technical experts, senior developers); o The cost of 1 person-day is set at 500 EUR.

Incurred by	Cost item	Data source	Data extrapolation
European Union	Update of the ECRIS technical specifications	• ECRIS technical specialist	• Cost estimates provided by ECRIS technical specialist. No data extrapolation technique applied. • Financial calculations done on the following basis: o Effort is estimated in person-days; o The cost estimates are based on the usage of senior persons (e.g. project manager, senior technical experts, senior developers); o The cost of 1 person-day is set at 500 EUR.
European Union	Update the ECRIS Reference Implementation	• ECRIS technical specialist	• Cost estimates provided by ECRIS technical specialist. No data extrapolation technique applied. • Financial calculations done on the following basis: o Effort is estimated in person-days; o The cost estimates are based on the usage of senior persons (e.g. project manager, senior technical experts, senior developers); o The cost of 1 person-day is set at 500 EUR.
European Union	Development of Reference Implementation for the national ECRIS TCN system	• ECRIS technical specialist	• Cost estimates provided by ECRIS technical specialist. No data extrapolation technique applied. • Financial calculations done on the following basis: o Effort is estimated in person-days; o The cost estimates are based on the usage of senior persons (e.g. project manager, senior technical experts, senior developers); o The cost of 1 person-day is set at 500 EUR.
European Union	ECRIS TCN management	• DG JUST	• Cost estimates provided by DG JUST. No data extrapolation technique applied.

Incurred by	Cost item	Data source	Data extrapolation
28 Member State	IT infrastructure for implementation of the national ECRIS TCN system	• Questionnaire answered by Member States • Data extrapolation technique	• Hardware update is not considered as an incremental assuming the reuse of hardware running ECRIS; • TESTA-ng connection is not considered as an incremental cost given that ECRIS already uses TESTA-ng; • For all inconsistent or missing data the following cost estimates were considered: o Software: ▪ Average Cost value calculated based on the information provide by vendors and confirmed by benchmarking with market prices: • Average Cost value: EUR 11 000 ▪ Average cost value was applied when data was not provided by a Member State and when the data provided was considered inconsistent (variation of more than 50% in relation to the average cost value). • Range of data considered consistent: Any value between EUR 5 500 and EUR 16 500. o Development: ▪ Average Cost value calculated based on the data provided by Member States using 'Truncated Mean' i.e. average value of data collected was calculated after discarding outliers. • Average Cost Value: 48 person days (one-off cost) distributed among 2018, 2019 and 2020. ▪ Average cost value was applied when data was not provided by a Member State and when the data provided was considered inconsistent (variation of more than 50% in relation to the average cost value). • Range of data considered consistent: Any value between 24 and 72 person days. o Maintenance: ▪ Average Cost value calculated based on the data provided by Member States using 'Truncated Mean' i.e. average value of data collected was calculated after discarding outliers. • Average Cost Value: 24 person days (ongoing cost) per year from 2022 to 2027. ▪ Average cost value was applied when data was not provided by a Member State and when the data provided was considered inconsistent (variation of more than 50% in relation to the average cost value). • Range of data considered consistent: Any value between 12 and 36 person days. o Support: ▪ Average Cost value calculated based on the data provided by Member States using 'Truncated Mean' i.e. average value of data collected was calculated after discarding outliers. • Average Cost Value: 12 person days (ongoing cost) per year from 2022 to 2021. ▪ Average cost value was applied when data was not provided by a Member State and when the data provided was considered inconsistent (variation of more than 50% in relation to the average cost value). • Range of data considered consistent: Any value between 6 and 18 person days.

Incurred by	Cost item	Data source	Data extrapolation
28 Member State	Setup of the national ECRIS TCN system	• AFIS Vendors • Data extrapolation technique • Benchmark with ECRIS	o Development: ▪ Average Cost value calculated based on the information provide by vendors and confirmed by benchmarking with market prices: • Average Cost value: EUR 125 000 per Member States spread over 3 years of system development o Maintenance: ▪ Average Cost value calculated based on the data provided by vendors using a multiplier of 20%. The assumption that yearly maintenance costs are equivalent to 20% of total development costs are widely applied in IT cost assessments in the market. • Average Cost Value: EUR 25 000 per Member State per year of system operation. o Support: ▪ Average Cost value calculated based on the benchmark with other decentralised Commission systems such as ECRIS. o Average Cost Value: EUR 20 000 per Member State per year of system operation.
28 Member State	National component for extracting and transmitting alphanumeric identity records and fingerprints	• Questionnaire answered by Member States • Data extrapolation technique	• One-off costs: o Average Cost value calculated based on the data provided by Member States using ‘Truncated Mean’ i.e. average value of data collected was calculated after discarding outliers. o Average Cost value: 80 person days (one-off cost) distributed among 2018, 2019, and 2020. o Average cost value was applied when data was not provided by a Member State and when the data provided was considered inconsistent (variation of more than 50% in relation to the average cost value). o Range of data considered consistent: Any value between 40 and 120 person days. • Ongoing costs: o Average Cost value calculated assuming that maintenance costs are equivalent to 20% of overall development costs. o Average Cost value: 16 person days (ongoing cost) per year from 2021 to 2026. o Average cost value was applied when data was not provided by a Member State and when the data provided was considered inconsistent (variation of more than 50% in relation to the average cost value). • Range of data considered consistent: Any value between 8 and 24 person days.
28 Member State	Update of national AFIS for verification following a hit in the central ECRIS TCN system	• AFIS Vendors • Data extrapolation technique	• Original data provided by specialised vendors for the setup of a new dedicated AFIS at national level. • The data was extrapolated by applying a multiplier of 40%. This is based on the assumption that the costs for updating the national AFIS would account on average 40% of development and software licenses of a new AFIS.

Annex IV. Detailed view on the cost estimates

Table 28 presents the estimated total costs in million EUR (to three decimal places) incurred by the European Union and by the 28 Member States, grouped by cost type (i.e. hardware, software, development, maintenance, and support) for all cost items composing the centralised ECRIS TCN solution.

Table 28 Cost aggregation for the establishment of a centralised ECRIS TCN solution

Incurred by	Cost item	Cost type (*in million EUR, to three decimal places)*	One-off costs (3 years)	Ongoing costs (1 year)
European Union	1 - IT infrastructure of the central ECRIS TCN system	Hardware	0,619	0,124
		Software	0,504	0,101
		Development	0,375	-
		Maintenance & Support[86]	-	0,060
	Total		1,498	0,285
European Union	2 - Central component for loading alphanumeric identity records and fingerprints	Hardware	-	-
		Software	-	-
		Development	0,200	-
		Maintenance & Support[86]	-	0,025
	Total		0,200	0,025
European Union	3 - Central alphanumeric search engine	Hardware	-	-
		Software	1,700	-
		Development	0,290	-
		Maintenance & Support[86]	-	0,340
	Total		1,990	0,340
European Union	4 - Central AFIS system component	Hardware	0,810	-

[86] Data collected does not allow for the break down between maintenance and support costs. Therefore the values presented refer to both support and maintenance costs.

Incurred by	Cost item	Cost type (*in million EUR, to three decimal places)*	One-off costs (3 years)	Ongoing costs (1 year)
		Software	2,650	-
		Development	1,640	-
		Maintenance & Support[87]	-	0,720
	Total		5,100	0,720
European Union	5 - Central component for monitoring and analytics	Hardware	-	-
		Software	-	-
		Development	0,150	-
		Maintenance & Support[87]	-	0,030
	Total		0,150	0,030
European Union	6 – Technical specification for the ECRIS TCN solution	Hardware	-	-
		Software	-	-
		Development	0,190	-
		Maintenance	-	-
		Support	-	-
	Total		0,190	-
European Union	7 - Update of the ECRIS technical specifications	Hardware	-	-
		Software	-	-
		Development	0,067	-
		Maintenance	-	-
		Support	-	-
	Total		0,067	-
European Union	8 – Update the ECRIS Reference Implementation	Hardware	-	-
		Software	-	-

[87] Data collected does not allow for the break down between maintenance and support costs. Therefore the values presented refer to both support and maintenance costs.

Incurred by	Cost item	Cost type (*in million EUR, to three decimal places)*	One-off costs (3 years)	Ongoing costs (1 year)
		Development	0,259	-
		Maintenance	-	-
		Support	-	-
	Total		0,259	-
European Union	9 - Development of Reference Implementation for the national ECRIS TCN system	Hardware	-	-
		Software	-	-
		Development	1,046	-
		Maintenance & Support[88]	-	0,209
	Total		1,046	0,209
European Union	10 - ECRIS TCN management	Development	2,762	
		Maintenance & Support[88]		0,476
	Total		2,762	0,476
European Union	Total for the European Union		13,262	2,085
28 Member State	11 - IT infrastructure for implementation of the national ECRIS TCN system	Hardware	0,306	-
		Software[89]	-	-
		Development	0,208	-
		Maintenance	-	0,100
		Support	-	0,052
	Total		0,514	0,152
28 Member State	12 - National component for extracting and transmitting alphanumeric identity records and fingerprints	Hardware	-	-
		Software	-	-
		Development	0,342	-
		Maintenance	-	0,075

[88] Data collected does not allow for the break down between maintenance and support costs. Therefore the values presented refer to both support and maintenance costs.

[89] All COTS software used to run the national ECRIS TCN Reference Implementation are open software. Therefore, there is no incremental costs for software licenses.

Incurred by	Cost item	Cost type (*in million EUR, to three decimal places)*	One-off costs (3 years)	Ongoing costs (1 year)
		Support	-	-
	Total		0,342	0,075
28 Member State	13 – Setup of the national ECRIS TCN system	Hardware	-	-
		Software	-	-
		Development	3,500	-
		Maintenance	-	0,700
		Support	-	0,560
	Total		3,500	1,260
28 Member State	14 - Update of national AFIS for verification following a hit in the central ECRIS TCN system	Hardware	-	-
		Software	2,648	-
		Development	6,340	-
		Maintenance	-	-
		Support	-	-
	Total		8,988	-
28 Member States	Total for the 28 Member States		13,344	1,487
	Total for the European Union and 28 Member States		26,606	3,571