Final Report

Feasibility study on the inclusion of pseudonymised fingerprints in ECRIS TCN exchanges

30 June 2016

This report was carried out for the European Commission Directorate-General for Justice and Consumers by:

Authors:

KURT SALMON: Debora Di Giacomo and Stefan Georgiev

INTRASOFT: Ludovic Colacino Dias

GLSI: Gary Linton, Nicholas Apps, Anja Harris, Richard Garner, and Ian Gledhill

Internal Identification:
Specific Contract No: 308
Framework Contract: DI/07172 - ABCIII

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.

© European Union, 2016

Table of Contents

EXECUTIVE SUMMARY **11**

INTRODUCTION **14**

1 CONTEXT AND BACKGROUND **16**

2 DEFINITIONS **18**

2.1.1 Pseudonymisation *18*

2.1.2 Third Country Nationals (TCN) *18*

3 STATE OF PLAY CONCERNING PSEUDONYMISATION OF FINGERPRINTS **19**

3.1 PARTICULARITIES OF THE BIOMETRIC TEMPLATE PROTECTION TECHNIQUES 19

3.2 AVAILABLE MARKET SOLUTIONS 20

3.3 RESEARCH FINDINGS REGARDING PSEUDONYMISATION OF FINGERPRINTS 21

3.3.1 Findings of Joint Research Centre of the European Commission *21*

3.3.2 Findings of the TURBINE research project *22*

3.4 ALTERNATIVE PSEUDONYMISATION STRATEGY 23

3.5 SUMMARY OF FINDINGS ON PSEUDONYMISATION OF FINGERPRINTS 24

4 STATE OF PLAY REGARDING THE USE OF FINGERPRINTS IN EUROPEAN SYSTEMS **25**

4.1 EURODAC 25

4.2 VISA INFORMATION SYSTEM (VIS) 25

4.3 SCHENGEN INFORMATION SYSTEM (SIS) 26

4.4 PRÜM ARRANGEMENTS 27

4.5 INTERPOL AFIS SYSTEM 28

5 STATE OF PLAY REGARDING THE USE OF FINGERPRINTS IN MEMBER STATES **29**

5.1 IMPORTANT CONSIDERATIONS ON THE USE OF FINGERPRINTS FOR ECRIS TCN EXCHANGES 30

5.1.1 The size of the problem *30*

5.1.2 Availability and access to fingerprints *33*

5.1.3 Capturing of fingerprints *34*

5.1.4 Quality of fingerprints *35*

5.1.5 Matching of fingerprints *35*

6 TECHNICAL SCENARIOS **39**

6.1 DESCRIPTION OF SCENARIO 1: DECENTRALISED ECRIS TCN SYSTEM, SHARING OF FINGERPRINTS AND LOCAL "HIT/NO HIT" SEARCH 41

6.1.1 Description of Scenario 1A *42*

6.1.2 Description of Scenario 1B *49*

6.2 DESCRIPTION OF SCENARIO 2: DECENTRALISED ECRIS TCN SYSTEM, NO SHARING OF FINGERPRINTS AND DISTRIBUTED "HIT/NO HIT" SEARCH 53

6.2.1 Description of Scenario 2A *54*

6.2.2 Description of Scenario 2B *60*

6.3 DESCRIPTION OF SCENARIO 3: CENTRAL AFIS, SHARING OF ALPHANUMERIC DATA, "HIT/NO HIT" SEARCH AT CENTRAL AND LOCAL LEVEL 64

6.3.1 Description of Scenario 3A *65*

6.3.2 Description of Scenario 3B *70*
6.4 DESCRIPTION OF SCENARIO 4: CENTRAL ECRIS TCN SYSTEM, FULLY CENTRALISED "HIT/NO HIT" SEARCH 75
6.4.1 Description of Scenario 4A *76*
6.4.2 Description of Scenario 4B *81*
6.5 TECHNICAL AND OPERATIONAL IMPACTS OF THE SCENARIOS 86
7 COSTS ASSOCIATED WITH THE TECHNICAL SCENARIOS 92
7.1 METHODOLOGY 92
7.1.1 Step I: Define the scope of the ICT Cost Assessment *93*
7.1.2 Step II: Prepare the ICT Cost Assessment *94*
7.1.3 Step III: Assess the ICT impacts *98*
7.2 COST ASSESSMENT OF THE TECHNICAL SCENARIOS 99
7.2.1 General assumptions *99*
7.2.2 Cost assessment of Scenarios 1A & 1B *101*
7.2.3 Cost assessment of Scenarios 2A & 2B *108*
7.2.4 Cost assessment of Scenarios 3A & 3B *115*
7.2.5 Cost assessment of Scenarios 4A & 4B *121*
7.3 COMPARISON OF THE COSTS FOR IMPLEMENTATION OF THE TECHNICAL SCENARIOS 127
7.3.1 Cost comparison for the inclusion of pseudonymised fingerprints *127*
7.3.2 Cost comparison for the inclusion of pseudonymised fingerprints and alphanumeric data 128
8 CONCLUSIONS 131
9 ANNEXES 133
ANNEX 1. ADMINISTRATIVE COSTS 133
General assumptions *133*
Administrative activities performed for the ECRIS TCN exchanges *133*
Detailed calculation *135*
ANNEX 2. DISTRIBUTION OF COST PER MEMBER STATE 141
ANNEX 3. VOLUMETRIC AND FINGERPRINTS SIZING INFORMATION FOR THE ECRIS TCN EXCHANGES ... 144
General assumptions on TCN fingerprint processing and storage *144*
Estimated volume of TCN fingerprint processing and storage *145*
Estimated volume and storage of TCN fingerprints for Scenario 1 ..... *147*
Estimated volume and storage of TCN fingerprints for Scenario 2 ..... *148*
Estimated volume and storage of TCN fingerprints for Scenarios 3 and 4 ..... *150*
ANNEX 4. COUNTRY FICHE ON THE STATE OF PLAY OF FINGERPRINTS USAGE 153
ANNEX 5. WORKSHOP ON PSEUDONYMISATION OF FINGERPRINTS – EUROPEAN COMMISSION, BRUSSELS, 15 MARCH 2016 157
ANNEX 6. DETAILED VIEW ON THE COST ESTIMATES 158

List of figures

Figure 1 Problem tree for ECRIS TCN 16
Figure 2 Number of TCN convictions per year in the EU (19 Member States) 31
Figure 3 Number of TCN convictions in the EU in 2014 33
Figure 4 Number of tenprints stored in National AFIS as of 2014 36
Figure 5 Percentage breakdown of number of tenprints held in national AFIS systems 36
Figure 6 Overview of Scenario 1A 43
Figure 7 Process for a new conviction of a TCN in Scenario 1A 44
Figure 8 Process for dissemination of TCN identity information in Scenario 1A 45
Figure 9 Process for local “hit/no hit” search in Scenario 1A 47
Figure 10 Process for ECRIS request in Scenario 1A 48
Figure 11 Overview of Scenario 1B 49
Figure 12 Process for new conviction of a TCN in Scenario 1B 50
Figure 13 Process for dissemination of TCN identity information in Scenario 1B 51
Figure 14 Process for local “hit/no hit” search in Scenario 1B 52
Figure 15 Process for ECRIS request in Scenario 1B 53
Figure 16 Overview of Scenario 2A 55
Figure 17 Process for new conviction of a TCN in Scenario 2A 56
Figure 18 Process for dissemination of TCN identity information in Scenario 2A 57
Figure 19 Process for distributed “hit/no hit” search in Scenario 2A 58
Figure 20 Process for ECRIS request in Scenario 2A 59
Figure 21 Overview of Scenario 2B 60
Figure 22 Process for new conviction of a TCN in Scenario 2B 61
Figure 23 Process for dissemination of TCN identity information in Scenario 2B 62
Figure 24 Process for distributed “hit/no hit” search in Scenario 2B 63
Figure 25 Process for ECRIS request in Scenario 2B 64
Figure 26 Overview of Scenario 3A 66
Figure 27 Process for new conviction of a TCN in Scenario 3A 67
Figure 28 Process for dissemination of TCN identity information in Scenario 3A 68
Figure 29 Process for central and local “hit/no hit” search in Scenario 3A 69

Figure 30 Process for ECRIS request in Scenario 3A 70
Figure 31 Overview of Scenario 3B 71
Figure 32 Process for new conviction of a TCN in Scenario 3B 72
Figure 33 Process for dissemination of TCN identity information in Scenario 3B 73
Figure 34 Process for central and local “hit/no hit” search in Scenario 3B 74
Figure 35 Process for ECRIS request in Scenario 3B 75
Figure 36 Overview of Scenario 4A 77
Figure 37 Process for new conviction of a TCN in Scenario 4A 78
Figure 38 Process for dissemination of TCN identity information in Scenario 4A 79
Figure 39 Process for central “hit/no hit” search in Scenario 4A 80
Figure 40 Process for ECRIS request in Scenario 4A 81
Figure 41 Overview of scenario4B 82
Figure 42 Process for new conviction of a TCN in Scenario 4B 83
Figure 43 Process for dissemination of TCN identity information in Scenario 4B 84
Figure 44 Process for central “hit/no hit” search in Scenario 4B 85
Figure 45 Process for ECRIS request in Scenario 4B 86
Figure 46 ICT Cost Assessment Overall Approach 92
Figure 47 Labour Daily Rates per MS in Euro 100
Figure 48 Scenario 1A & 1B: Total costs for Fingerprints (1/2) 107
Figure 49 Scenario 1A & 1B: Total costs for Fingerprints (2/2) 108
Figure 50 Scenario 2A & 2B: Total costs for Fingerprints (1/2) 114
Figure 51 Scenario 2A & 2B: Total costs for Fingerprints (2/2) 115
Figure 52 Scenario 3A & 3B: Total costs for Fingerprints (1/2) 120
Figure 53 Scenario 3A & 3B: Total costs for Fingerprints (2/2) 121
Figure 54 Scenario 4A & 4B: Total costs for Fingerprints (1/2) 126
Figure 55 Scenario 4A & 4B: Total costs for Fingerprints (2/2) 126
Figure 56 Cost comparison for Fingerprints for EU and 28 MS (1/2) 128
Figure 57 Cost comparison for Fingerprints for EU and 28 MS (2/2) 128
Figure 58 Cost comparison for Fingerprints and Alphanumeric Data for the EU and 28 MS (1/3) 129
Figure 59 Costs’ comparison for Fingerprints and Alphanumeric Data for the EU and 28 MS (2/3) 130
Figure 60 Cost comparison for Fingerprints and Alphanumeric Data for the EU and 28 MS (3/3) 130

Figure 61 Administrative costs for Scenarios 1A, 1B, 2A, 2B, 3B, and 4B (30% searches) 137

Figure 62 Administrative costs for Scenarios 1A, 1B, 2A, 2B, 3B, and 4B (100% searches) 138

Figure 63 Administrative costs for Scenario 3A and 4A (30% searches).....139

Figure 64 Administrative costs for Scenario 3A and 4A (100% searches).....140

Figure 65 Total Administrative costs per year.....140

Figure 66 One-off costs per Member State for fingerprints according to the number of TCN convictions/year 141

Figure 67 Yearly recurring costs per Member State for fingerprints according to the number of TCN convictions/year 142

Figure 68 Alphanumeric costs for Scenarios 1A, 1B, 2A, 2B, 3A, and 3B 143

Figure 69 Alphanumeric costs for Scenarios 4A and 4B.....143

List of tables

Table 1 Alternative pseudonymisation strategies and their impact on ECRIS TCN exchanges 23

Table 2 Number of convicted TCN (in thousands) provided through several surveys 32

Table 3 Authorities with access to the national AFIS system[37] 34

Table 4 Summary of the stakeholder groups 93

Table 5 Technical scenarios and related cost items and ICT cost categories 96

Table 6 Scenario 1A: Cost elements.....102

Table 7 Scenario 1A: Total costs summary (Fingerprints) 104

Table 8 Scenario 1B: Cost elements.....105

Table 9 Scenario 1B: Total costs summary (Fingerprints) 107

Table 10 Scenario 2A: Cost elements.....109

Table 11 Scenario 2A: Total costs summary (Fingerprints) 111

Table 12 Scenario 2B: Cost elements.....112

Table 13 Scenario 2B: Total costs summary (Fingerprints) 114

Table 14 Scenario 3A: Cost elements.....116

Table 15 Scenario 3A: Total costs summary (Fingerprints) 117

Table 16 Scenario 3B: Cost elements.....118

Table 17 Scenario 3B: Total costs summary (Fingerprints) 120

Table 18 Scenario 4A: Cost elements.....122

Table 19 Scenario 4A: Total costs summary (Fingerprints) 123

Table 20 Scenario 4B: Cost elements.....124

Table 21 Scenario 4B: Total costs summary (Fingerprints) 125

Table 22 Overall evaluation of ECRIS TCN Technical Scenarios.....131

Table 23 Administrative activities performed for the ECRIS TCN exchanges 134

Table 24 Frequency and duration of the administrative activities 135

Table 25 Administrative costs of ECRIS TCN for Scenario 1A, 1B, 2A, 2B, 3B, and 4B 136

Table 26 Administrative costs of ECRIS TCN for Scenario 3A and 4A.....138

Table 27 Member States categorised according to the number of TCN convictions per year 141

Table 28 Estimated number of ECRIS requests for TCN.....146

Table 29 Estimated number of processing operations – Scenario 1 (low).....147

Table 30 Estimated number of processing operations – Scenario 1 (medium) 147

Table 31 Estimated number of processing operations – Scenario 1 (high) 148

Table 32 Estimated volume for storage, cumulative over 5 years – Scenario 1 (all Member States).....148

Table 33 Estimated number of processing operations – Scenario 2 (low).....149

Table 34 Estimated number of processing operations – Scenario 2 (medium) 149

Table 35 Estimated number of processing operations – Scenario 2 (high) 149

Table 36 Estimated volume for storage, cumulative over 5 years – Scenario 2 (low) 149

Table 37 Estimated volume for storage, cumulative over 5 years – Scenario 2 (medium) 149

Table 38 Estimated volume for storage, cumulative over 5 years – Scenario 2 (high) 150

Table 39 Estimated number of processing operations (low) 150

Table 40 Estimated number of processing operations (medium).....150

Table 41 Estimated number of processing operations (high).....151

Table 42 Estimated volume for storage, cumulative over 5 years (low).....151

Table 43 Estimated volume for storage, cumulative over 5 years (medium) 151

Table 44 Estimated volume for storage, cumulative over 5 years (high) 151

Table 45 Estimated number of processing operations (central AFIS).....151

Table 46 Estimated volume for storage, cumulative over 5 years (central AFIS) 151

Table 47 Country Fiches on the State of Play of fingerprints usage 153

Table 48 Cost distribution per type for the inclusion of Fingerprints in ECRIS TCN exchanges.....158

Table 49 Cost distribution per cost element for the inclusion of Fingerprints in ECRIS TCN exchanges ...160

Revision History

The following table shows the development of this document.

Date	Version	Description	Author(s)	Reviewed by
03.03.2016	V0.1 – V0.2	First draft released and updated version followed after a review by DG JUST.	Stefan Georgiev Debora Di Giacomo Anja Harris	Nicholas Apps Gary Linton, Nicholas Apps Ian Gledhill
01.04.2016	V0.3 – V0.5	Information added to all sections of the document, especially part II and III.	Richard Garner Ian Gledhill Anja Harris Gary Linton, Nicholas Apps	Anja Harris Nicholas Apps Gary Linton Richard Garner Ian Gledhill
07.04.2016	V0.6	Updates to all sections and comments' incorporation, received from Debora di Giacomo and DG JUST.	Anja Harris	Nicholas Apps Gary Linton, Nicholas Apps Ian Gledhill
12.04.2016	V0.7 – V0.8	Amendment to section 4 (technical scenarios) as discussed in progress meeting on 12 April 2016.	Nicholas Apps Gary Linton	Anja Harris Ian Gledhill Richard Garner
13.04.2016	V0.8	Initiation of the ICT Cost Assessment chapter.	Stefan Georgiev	Debora Di Giacomo
29.04.2016	V0.9 – V0.10	Editing all sections based on comments received by Ludovic Colacino-Dias, Nicholas Apps and DG JUST.	Anja Harris Gary Linton	Anja Harris Gary Linton
05.05.2016 - 31.05.2016	V0.11 – V0.22	Overall edits and additional work on Section 5 (Cost associated with the scenarios).	Stefan Georgiev Debora Di Giacomo Anja Harris	Debora Di Giacomo
01.06.2016	V1.00	Final Report submitted for a review to DG JUST (description of the technical scenarios is not included in this version).	Stefan Georgiev Debora Di Giacomo	Debora Di Giacomo
01.06.2016 - 16.06.2016	V1.01 – V1.12	Internal reviews implementing the comments received from DG JUST.	Stefan Georgiev Debora Di Giacomo Nicholas Apps Gary Linton Ludovic Colacino Dias	Debora Di Giacomo
17.06.2016	V2.00	Updated version submitted to DG JUST for review.	Stefan Georgiev Debora Di Giacomo Ludovic Colacino Dias Nicholas Apps Gary Linton	Djamila Ben Miloud Jaime Lopez Loosvelt Haryo Nindito
21.06.2016	V3.00	Updated version submitted to DG JUST for review.	Stefan Georgiev Debora Di Giacomo Ludovic Colacino Dias Nicholas Apps Gary Linton	Dick Heimans Djamila Ben Miloud Haryo Nindito
29.06.2016	V4.09 – 4.17	Internal reviews and updates	Stefan Georgiev Debora Di Giacomo Ludovic Colacino Dias	Jaime Lopez Loosvelt Haryo Nindito
30.06.2016	V5.00	Final version approved by DG JUST	Stefan Georgiev Debora Di Giacomo	Dick Heimans Jaime Lopez Loosvelt Haryo Nindito

Executive Summary

The European Criminal Record Information System (ECRIS) is a decentralised system for electronic exchange of criminal record information. The system works effectively for EU nationals. However, regarding Third Country Nationals or Stateless person (TCN), Member States cannot know which Member States to contact with requests for criminal record information, thus resulting in either blanket searches or in no exchanges of information.

A reliable system for the exchange of information on convictions requires a sufficient degree of certainty regarding the data identifying a specific person. Identity criteria currently used in ECRIS rely on alphanumeric identity information (e.g. name of the person, the father's name, the mother's name, date and place of birth, nationality, country of birth, etc.) and fingerprints. Establishing the identity of TCN without fingerprints can be challenging because of the use of different alphabets, languages, common surnames or because reliable identity documents are not available.

Against this background, the Commission has launched a legislative proposal[1] to implement a mechanism where Member States could easily identify Member State(s) in which TCN have already been convicted, so that criminal record information requests can be addressed to the correct Member State. The proposal foresees the mandatory inclusion of fingerprints in the ECRIS TCN exchanges.

In the implementation scenarios described under section 6 of this study it is proposed to disseminate the fingerprints of convicted TCN. Ensuring the secured and protected distribution of ECRIS TCN information is essential in order to gain trust and acceptance, both from the ECRIS practitioners and the citizens. One of the objectives of this study is to analyse and assess the privacy-protection techniques to pseudonymise fingerprints so that they can be distributed in a secure way. This feasibility study explores the state of play concerning the pseudonymisation of fingerprints, both in terms of available solutions in the market and research. Proven techniques for protecting alphanumeric information, such as the one used in Ma3tch[2], cannot be used to pseudonymise fingerprints. Whilst there are a number of fingerprints pseudonymisation techniques, offering varying levels of privacy protection, the findings of this study confirmed that the most advanced ones are not suitable for large scale systems such as ECRIS. Other studies such as the one carried out by the Joint Research Centre[3] of the European Commission have also arrived at this conclusion when exploring a fingerprint matching functionality for ECRIS. Furthermore, no market solutions for advanced pseudonymisation of fingerprints in a large scale context are available.

---

[1] 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, Brussels, 19 January 2016.

[2] Ma^{3}tch (Autonomous Anonymous Analysis Matching) has been recently introduced in the FIU network. Ma^{3}tch is based on a technology which aims at improving the exchange of sensitive information by excluding unnecessary requests, improving timeliness and enhancing privacy. Financial Intelligence Units (FIUs) are EU central, national intelligence agencies responsible for receiving, analysing and disseminating disclosures of financial information to the competent authorities (e.g., law enforcement or prosecutorial authorities) in order to combat money laundering and terrorism financing (www.fiu.net).

[3] Joint Research Centre of the European Commission, Note on an AFIS functionality for the European Criminal Records Information System: A preliminary assessment of DG JUST decentralised option supported by pseudonymised index-filter, 9 February 2016, published on https://ec.europa.eu/jrc/en/publications-list.

There are however alternative pseudonymisation strategies which are based on the removal of biographical identity data from fingerprints. These strategies are suitable for large scale environments such as ECRIS and are the ones considered in the legislative proposal and in the implementation scenarios described under section 6 of this study.

The study also focused on the use of fingerprints in European systems and the use of pseudonymisation techniques in such systems. A number of comparable fingerprint identification systems, such as EURODAC (European identification system for asylum applicants), the Visa Information System (VIS), the Schengen Information System (SIS) and the decentralised Prüm fingerprint searching arrangements, were considered. Even though it is not an EU system, Interpol's Automated Fingerprint Identification System (AFIS) was considered for completeness.

As part of this feasibility study, a number of research activities and Member State visits were conducted in order to establish the state of play regarding the use of fingerprints in all Member States. The research revealed that the vast majority of Member States have existing automated fingerprint matching systems managed by law enforcement authorities, while ECRIS exchanges are under the responsibility of judicial authorities. Also there are a variety of fingerprint matching solutions throughout the EU, which utilise different quality thresholds for matching fingerprints. Finally, the research demonstrated that there is a variety of fingerprint capturing processes employed across the EU, and consequently the quality of fingerprints stored at national and European level varies too.

This study considered two options as the most realistic and feasible for the inclusion of pseudonymised fingerprints in the exchange of TCN convictions: a decentralised "hit/no hit" option and a central "hit/no hit" option. Both options require the establishment of an automated system holding identification data for convicted TCN.

The two options identified for establishing an ECRIS TCN system have been split into a set of four technical scenarios, with variants described as follows:

- Decentralised "hit/no hit" option:
    - Scenario 1A: Sharing of fingerprints and alphanumeric identity data of convicted TCN with all other Member States, local hit/no hit search and use of a dedicated national AFIS for searching purposes;
    - Scenario 1B: Sharing of fingerprints and alphanumeric identity data of convicted TCN with all other Member States, local hit/no hit search and reuse or extension of an existing national AFIS for searching purposes;
    - Scenario 2A: No sharing of fingerprints, only sharing of alphanumeric identity data with all other Member States, distributed "hit/no hit" search with fingerprints and use of a dedicated national AFIS for searching purposes;
    - Scenario 2B: No sharing of fingerprints, only sharing of alphanumeric identity data with all other Member States, distributed "hit/no hit" search with fingerprints and reuse or extension of an existing national AFIS for searching purposes;
- Central "hit/no hit" option:

- Scenario 3A: Central storage of fingerprints with a hit/no hit search of fingerprints for convicted TCN (AFIS), sharing of alphanumeric identity data with all other Member States, upon an ECRIS request verification of fingerprints is performed manually at national level without support of a national AFIS;
- Scenario 3B: Central storage of fingerprints with a hit /no hit search of fingerprints for convicted TCN (AFIS), sharing of alphanumeric identity data with all other Member States, upon an ECRIS request an existing national AFIS is used for verification of fingerprints;
- Scenario 4A: Central storage of both alphanumeric identity data and fingerprints of convicted TCN, central hit/no hit search (alphanumeric and AFIS), upon an ECRIS request verification of fingerprints is performed manually at national level without support of a national AFIS;
- Scenario 4B: Central storage of both alphanumeric identity data and fingerprints of convicted TCN, central hit/no hit search (alphanumeric and AFIS), upon an ECRIS request an existing national AFIS is used for verification of fingerprints.

The specificities of each technical scenario are analysed in this study and further described in section 6.

As a final step of the feasibility study, an ICT Cost Assessment was carried out, evaluating and comparing each technical scenario against estimated incurred costs. As a result, Scenario 3A (EUR 11.6 million), was evaluated as the less costly scenario to implement the ECRIS TCN system followed by Scenario 4A (EUR 16.7 million), while Scenario 1A (EUR 60.2 million) and 2A (EUR 48.6 million) are the most costly ones[4]. The study also analysed the technical and operational impacts of each technical scenario.

Overall, the study concluded that the technical, operational and cost impacts are better evaluated for the centralised scenarios 3 and 4. The centralised options are not only less costly but also less complex to implement compared to the decentralised options. In evaluating the complexity of the different options, the main consideration was that the implementation of the ECRIS TCN system could benefit from proven technologies and successful implementation of already existing fully automated centralised systems such as EURODAC and VIS. Decentralised options are also considered feasible for the implementation of ECRIS TCN exchanges, however at higher costs and higher complexity than the centralised options.

[4] All cost estimates presented in this study are estimates and do not represent any firm commitment.

Introduction

As stipulated in the Treaty on European Union[5], the Union shall offer its citizens an area of freedom, security and justice without internal frontiers. This objective presupposes the systematic efficient exchange, among the competent authorities of the Member States, of information extracted from criminal records in a way that would guarantee its common understanding[6].

In this context, the European Union established the European Criminal Records Information System (ECRIS)[7]. ECRIS is a system that aims at exchanging criminal records information among the 28 Member States in an electronic way. Operational since 2012, it ensures, that all previous convictions handed down in other Member States, are electronically exchanged in a timely manner.

ECRIS works efficiently with regard to EU nationals. However, the system does not ensure the exchange of complete information on previous convictions of Third Country Nationals and Stateless persons (hereafter TCN)[8]. Moreover, the European Agenda on Security[9] stresses the need to improve ECRIS with regard to convicted TCN as part of a coordinated response of Member States to the increasing treats of terrorism and cross-border crimes.

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.'[10]

[5] Consolidated version of the Treaty on European Union, Official Journal of the European Union, Brussels, 26 October 2012.
[6] 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, Official Journal of the European Union [L 93/33], Brussels, 7 April 2009.
[7] 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.
[8] A 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.
[9] 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 April 2015.
[10] European Commission - Press release, Commission proposes to strengthen the exchange of criminal records on non-EU citizens, Strasbourg, 19 January 2016.

On 19 January 2016, the Commission adopted a proposal[11] for a Directive amending Council Framework Decision 2009/315/JHA[12], regarding ECRIS and TCN, and replacing Council Decision 2009/316/JHA. The proposal foresees the inclusion of fingerprints in the exchanges of criminal records through ECRIS. Specifically the proposal also foresees the use of anonymisation techniques, referred as pseudonymisation in this study, to ensure that privacy protection concerns are adequately addressed.

As an input to the Commission's proposal, KURT SALMON conducted in 2015 an ICT cost assessment[13], evaluating the possible technical scenarios identified so far to exchange information regarding TCN without pseudonymised fingerprints. As a continuation of this study, the European Commission Directorate-General for Justice and Consumers (DG JUST) mandated KURT SALMON, in partnership with GLSI and INTRASOFT, to further assess the impact of the inclusion of pseudonymised fingerprints in ECRIS TCN exchanges.

This study aims at assessing the feasibility and costs of the inclusion of pseudonymised fingerprints in ECRIS TCN exchanges. The scope of this study includes; (i) the assessment of the feasibility, availability and maturity of existing fingerprint pseudonymisation technologies, (ii) a description of the technical scenarios and (iii) the assessment of the impacts regarding costs for the inclusion of fingerprints in ECRIS TCN exchanges.

This report is articulated around the following sections:

- Section 1 describes the context and background of this study;
- Section 2 presents the main definitions;
- Section 3 describes the state of play concerning pseudonymisation of fingerprints;
- Section 4 describes the state of play regarding the use of fingerprints in EU systems;
- Section 5 describes the state of play regarding fingerprints in the 28 Member States;
- Section 6 describes the technical scenarios assessed in this study;
- Section 7 describes the cost associated with the technical scenarios and presents a comparison among them;
- Section 8 presents the conclusions; and
- Section 9 presents the annexes with detailed information supporting this study.

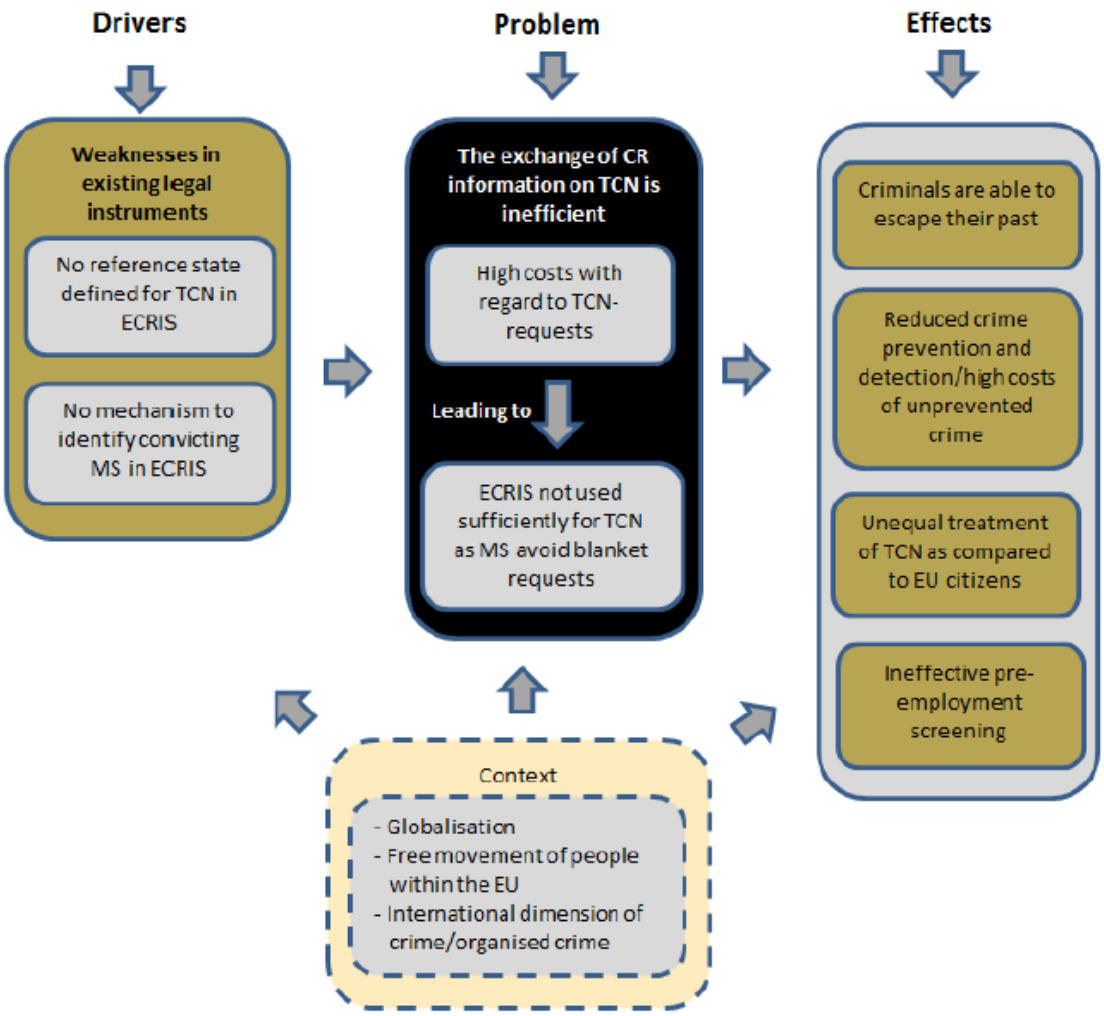
[11] Proposal for a Directive of The European Parliament and of The Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, Brussels, 19 January 2016.
[12] 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, Brussels, 7 April 2009.
[13] 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. Available at: http://ec.europa.eu/justice/criminal/files/ecris_tcn_ict_impact_assessment_final_report_en.pdf.

1 Context and background

The European Criminal Record Information System (ECRIS) is a decentralised system of electronic exchange of criminal record information. To date, 26 Member States exchange information using this system. The system works very well for EU nationals given that the Member State of nationality is the "reference" Member State for providing criminal records.

The current ECRIS legal framework does not sufficiently cover the particularities of requests concerning TCN. Although it is possible to exchange information on TCN through ECRIS, there is no procedure or mechanism in place to do so efficiently. As TCN have no Member State of nationality, in order to get a complete overview of their criminal history, a request must be directed to all Member States. Generally, the requesting Member States' authorities do not know in which Member State(s) a TCN has previously been convicted, which currently results in either blanket searches or no exchange of information. The figure below sets out the ECRIS TCN problem in the form of a problem tree:

Figure 1 Problem tree for ECRIS TCN[14]



[14] 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.

A reliable system for the exchange of information on convictions requires a sufficient degree of certainty regarding the data identifying a specific person. 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 identify 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 compulsory and optional information to be exchanged through ECRIS regarding requests on convicted persons. Regarding fingerprints, ECRIS provides for the exchange of fingerprints as a voluntary tool 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 according to national law.

Establishing the identity of 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. Against this background, the mandatory introduction into ECRIS of a fingerprint exchange and matching system is foreseen in the Commission's proposal.

2 Definitions

The following sections present two essential definitions for the understanding of this study.

2.1.1 Pseudonymisation

Directive (EU) 2016/680[15] gives the following definition for the term pseudonymisation as per Article 3(5):

> *'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.*

2.1.2 Third Country Nationals (TCN)

The proposed Directive to amend Council Framework Decision 2009/315/JHA (ECRIS TCN) proposes the following definition for TCN as per Article 2(e)[16]:

> *'third country national' means a national of a country other than a Member State, or a stateless person, or a person whose nationality is unknown to the Member State where a conviction is handed down against the person.*

It is important that the meaning of a TCN in this context is clearly defined, in order to ensure that the technical scenarios meet the business requirements of Member States. For example, the definition of TCN is subject to consideration whether or not to include persons with dual nationality, where one of the nationalities is that of an EU Member State (i.e. a national of at least one EU Member State and one non-EU state).

[15] EU Data Protection Directive: Article 3 (5) of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[16] 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.

3 State of play concerning pseudonymisation of fingerprints

It is foreseen in the proposed implementation scenarios described under section 6 to disseminate the alphanumeric identity information and the fingerprints of convicted TCN. Ensuring the secured and protected distribution of ECRIS TCN identity information is essential in order to gain trust and acceptance, both from ECRIS practitioners and citizens. Whilst privacy protection techniques, such as the one used in Ma3tch, may be suitable for the dissemination of alphanumeric identity information in ECRIS, they cannot be applied to fingerprints.

Fingerprints are collected under the form of images. A fingerprint image is unique and for this reason, contrary to a password, it cannot be replaced in case of unauthorised access. In order to be used within an automatic matching process, the fingerprint images are converted into a set of discriminative key features such as ridge terminations, ridge bifurcations and ridge angles. The complete set of discriminative features is known as a fingerprint template. In case of a leak of an unprotected fingerprint template the original image of the fingerprint can be recreated and misused.

Against this background, a number of protection techniques have been developed to prevent misuse of fingerprints and fingerprint templates. These are biometric[17] template protection techniques and considered as privacy enhancing techniques.

The remainder of this section presents the biometric template protection techniques to pseudonymise fingerprints so that they can be distributed in a more secure way, similar to the alphanumeric identity information, contributing to privacy and data protection requirements.

3.1 Particularities of the biometric template protection techniques

Given the sensitivity of sharing criminal records information and the expected high volume of exchanges, the most advanced biometric template protection techniques were explored.

Those techniques transform or convert fingerprint images into a protected file, called an encrypted template. Particular features of these advanced techniques include:

- the conversion is carried out in such a way that there is no way of recreating the original fingerprint image from the encrypted template: irreversibility;
- a large number of pseudonymised templates for the same fingerprints can be created for different purposes but cannot be linked: unlinkability; and
- the pseudonymised templates can be renewed or revoked: renewability.

[17] This study focuses only on fingerprints, not including any other biometrics.

In addition to these techniques and based on the conclusions of risk analyses on the system to be implemented, additional protecting measures can be taken such as the deletion of the original fingerprint images.

At present, the advanced template protection techniques fall into three major groups of emerging technologies: “Cryptobiometrics”, “cancellable biometrics” and “biometrics in the encrypted domain”. The features of these technologies look to provide enhanced data security and privacy.

Biometric cryptosystems is a group of emerging technologies that securely bind a digital key to a biometric data or generate a digital key from the biometric data, so that no biometric image or standard unprotected template is directly available. The key will be recreated only if the genuine biometric sample is presented on verification.

Cancellable Biometrics uses an irreversible feature transformation technique and stores the transformed template. On verification, the transformed templates are compared. This feature transformation implies a degradation of the system accuracy.

Biometrics in the encrypted domain schemes allow for computations to be performed on ciphertexts, with no additional auxiliary data (e.g., using Homomorphic Encryption), which generate encrypted results which decrypt to plaintexts that match the result of the operations carried out on the original plaintext.

Those techniques can be used in one-to-one (verification) and one-to-many (identification) matching process scenarios. Verification is a process where a new fingerprint image is taken from the user and is compared with the user's previously registered or stored fingerprints. This is done for example with fingerprint readers on smartphones or laptop devices. In an identification scenario, a fingerprint is taken from the user and compared to existing fingerprints of stored users in a database. Fingerprint identification requires searching in a database for a matched template and could result in a list of several candidates. It is a more complex and higher computationally demanding process than verification. Due to advancements in computing capabilities and the tremendous improvement of the accuracy level, identification has now become automated. The identification is nowadays performed by Automated Fingerprint Identification Systems (AFIS), which is a niche technology with only a few solution providers available on the world market. AFIS have been primarily used by law enforcement agencies for identification in criminal cases, and are now implemented in other areas of the society.

3.2 Available market solutions

The solutions currently available in the market apply one-to-one matching techniques to pseudonymised fingerprint templates. AFIS vendors[18] confirmed that there are no other options than applying one-to-one matching techniques to large scale systems as there are not yet acceptable one-to-many matching techniques applicable to pseudonymised fingerprint templates. Applying a one-to-one matching technique in a large scale system requires the matching process to be repeated many times against all fingerprints stored. As a result, each fingerprint search would take a significant amount of time.

[18] Workshop with Fingerprint (AFIS) vendors held at the Commission premises in Brussels on 15 March 2016.

Although satisfactory performances have been reported for one-to-one matching processes, when extending these to a one-to-many matching process, independently whether the fingerprints are protected or not, the accuracy performance drops significantly. The resulting large amount of errors would considerably challenge the use of a large scale system, which would be hard to accept by practitioners.

Another key disadvantage of privacy protection techniques described above, aside from the additional complexity that they bring, is that they create a vendor lock-in, since the pseudonymised fingerprint templates can only be matched using a vendor-specific matching technique. Consequently, it becomes difficult to change the selected protection technique to a different, potentially more accurate, efficient or cost effective fingerprint protection technique.

3.3 Research findings regarding pseudonymisation of fingerprints

Research projects indicate that one of the most significant issues with the current fingerprint template protection techniques is the detrimental impact on matching accuracy.

This section describes the most relevant research findings regarding pseudonymisation of fingerprints based on a study performed by the Joint Research Centre of the European Commission and on the TURBINE research project.

3.3.1 Findings of Joint Research Centre of the European Commission

A report from the Joint Research Centre of the European Commission stated the following[19]:

> *"protected biometric systems that enhance user's privacy should present an accuracy which is comparable to the one obtained by standard un-protected systems."*

Furthermore, in regards to performance aspects the report[20] draws the same conclusions, also confirmed by several fingerprint solution providers[21]:

> *"The current proposal for the inclusion of an AFIS within ECRIS, based on a decentralized architecture with a pseudonymised index-filter shared by all MS, presents severe flaws that will most likely lead to a failure of the fingerprint-based search engine. The pseudonymised dimension of the index-filter has been identified as the element of the proposal that will jeopardize the performance of the envisaged system new AFIS."*

[19] Joint Research Centre of the European Commission: Note on an AFIS functionality for the European Criminal Records Information System: A preliminary assessment of DG JUST decentralised option supported by pseudonymised index-filter, 9 February 2016, published on https://ec.europa.eu/jrc/en/publications-list.
[20] Joint Research Centre of the European Commission: Note on an AFIS functionality for the European Criminal Records Information System: A preliminary assessment of DG JUST decentralised option supported by pseudonymised index-filter, 9 February 2016, published on https://ec.europa.eu/jrc/en/publications-list.
[21] Fingerprints solution providers (AFIS) workshop held at European Commission, DG JUSTICE and CONSUMERS on 15 March 2016.

And

> *"The biometric protection template as suggested for the pseudonymisation of the fingerprints seems not to have reached the Technology Level Readiness which can be expected for ECRIS and will therefore not offer the required accuracy and processing time performance."*[22]

Reaching the same conclusions, the Biometric Institute[23] confirmed as well that the use of template protection techniques for large-scale one-to-many scenarios was so far not advised.

3.3.2 Findings of the TURBINE research project

The aim of the TURBINE (TrUsted Revocable Biometric IdeNtitiEs) research project was to provide a privacy enhancing technology, combining innovative developments in cryptography and fingerprint biometrics. Its aims were to provide highly reliable biometric one-to-one verifications, multi-vendor interoperability and system security, while solving issues related to privacy concerns associated to the use of biometrics for ID management. Its primary objective was to render this innovation commercially viable by demonstrating that the technology was sufficiently mature for deployment as a solution to large scale eID requirements. To achieve this, it was proposed to develop and evaluate the foundation and application of revocable protected biometric templates and pseudo-identities using fingerprint data. Use of different biometric enrolment algorithm transformations, and hence subsequent verification mechanisms, were to be evaluated against public and private fingerprint databases. Specific objectives were to ensure that the crypto-protection deployed on the biometric data was non-invertible and had the lowest possible impact.

The results of the performance evaluation of the fingerprint verification techniques in the context of the TURBINE project indicated that the development of privacy preserving technology for fingerprints was very challenging. The tests showed very significant performance deterioration at the pseudo-identity (protected) level test scenarios with respect to the unprotected systems which made the accuracy at the protected level very far from the initial targeted one. Several reasons were cited for this poor performance, among them: the small size of the database and the poor fingerprint image quality as the database was collected under not optimal conditions.

The overall conclusion of the TURBINE project after the tests was that it would be quite challenging to achieve the project's target performance, especially at the pseudo identity (protected) level. This was just covering the potentially simpler one-to-one verification scenario. The scope of TURBINE did not extend to the more challenging one-to-many identification scenario. The TURBINE project ended in 2011.

---

[22] Joint Research Centre of the European Commission: Note on an AFIS functionality for the European Criminal Records Information System: A preliminary assessment of DG JUST decentralised option supported by pseudonymised index-filter, 9 February 2016, published on https://ec.europa.eu/jrc/en/publications-list.

[23] The Biometrics Institute promotes the responsible use of biometrics as an independent and impartial international forum for biometric users and other interested parties. http://www.biometricsinstitute.org/.

3.4 Alternative pseudonymisation strategy

There are other protection strategies that do not suffer the same degree of degradation in performance and accuracy as the most advanced ones described earlier. If such strategies are accompanied with common security measures such as encryption, they have the potential to fully satisfy security and data protection requirements for ECRIS TCN exchanges. Table 1 below describes a range of alternative strategies to provide a level of pseudonymisation for fingerprint exchange, where encryption of the fingerprint template would not be required. However, it should be stressed that common IT protection measures can and must be applied in parallel.

Table 1 Alternative pseudonymisation strategies and their impact on ECRIS TCN exchanges

Strategies	Example usage of strategy	Impacts for ECRIS TCN
Provide fingerprint images in NIST format, with a reference number only, into a shared, searchable fingerprint index	EURODAC is an example of an EU AFIS solution that takes this approach	Avoids vendor lock-in and maximises flexibility and compatibility with existing national Member States AFIS systems, which are able to generate their own choice of templates. Sharing of a reference number, with the link to the real person identity details known to the originating Member State only, is considered in most existing EU solutions to have “pseudonymised” the data provided. This is supported by the Biometrics Institute who suggests that once metadata such as name, height, weight, date of birth and place of birth have been removed, fingerprints are inherently pseudonymised.
Use only fingerprint images without biographical data stored in a national Member States AFIS and provide a search capability into the AFIS from other Member States	The Prüm arrangement is an example of an EU fingerprint sharing solution that takes this approach	Avoids vendor lock-in and maximises flexibility and compatibility with existing national AFIS systems, which are able to generate their own choice of templates for local matching to suit. The incoming search requests have fingerprint images without biographical data with a reference number associated with them, with the link to the real person identity details known to the originating Member State only. This is considered in most existing EU solutions to have “pseudonymised” the data provided. In addition, the full database of one Member State is never shared with another Member State as the main database being searched against is held within the destination Member State database. The requirement to comply with privacy and data protection for this database resides with that Member State.
Provide standard ISO templates, with a reference number only, into a shared, searchable fingerprint index.	Use of standard ISO templates, or similar FBI standardisation approaches, has been used in the US since 2005[24]. This approach is not used currently in the context of EU wide sharing of fingerprint data.	Avoids risk of vendor lock-in and provides a solution capable of working with different AFIS solutions from different vendors but at a cost of impacting the higher accuracy that would be available from proprietary vendor's templates. In addition, changes to some national AFIS systems would likely be needed to be able to generate and support ISO templates. Sharing of a reference number, with the link to the real person identity details known to the originating Member States only, is considered in most existing EU solutions to have “pseudonymised” the data provided. Some may consider sharing of templates more acceptable than sharing fingerprint images themselves from a privacy/data protection point of view.

[24] ISO/IEC 19794-2:2005; ISO/IEC 19794-2:2011; ANSI/INCITS 378.

Strategies	Example usage of strategy	Impacts for ECRIS TCN
Provide vendor specific templates, with a simple reference number only, into a shared, searchable fingerprint index	This approach is not used currently in the context of EU wide sharing of fingerprint data	Risks vendor lock-in and would only work in a solution where all national AFIS systems are able to generate and support the same proprietary templates. Improves the maximum accuracy that would be available from ISO templates. Sharing of a reference number, with the link to the real person identity details known to the originating Member State only, is considered in most existing EU solutions to have "pseudonymised" the data provided. Sharing of templates is usually considered more privacy friendly[25] than sharing fingerprint images themselves from a privacy/data protection point of view.

Regarding the available alternative strategies based solely on the usage of fingerprint templates, it must be noted that in such cases it is not possible to perform manual comparisons and resolve 'grey area' responses (possible matches). This has significant implications for setting the appropriate thresholds for the fingerprint matching techniques and providing confidence of results. It means that any template only based solution can only operate in a so called 'lights out' automated mode with very high confidence matches. Subsequently template only based solutions have a higher chance of missing a potential match that would have fallen into the 'grey area'.

3.5 Summary of findings on pseudonymisation of fingerprints

Proven techniques for protecting alphanumeric information, such as the one used in Ma3tch, cannot be used to pseudonymise fingerprint images. A detailed examination of the particularities of the most advanced available techniques has explored accuracy and performance.

Overall, there are a number of advanced pseudonymisation techniques which use encryption algorithms for protecting fingerprints, but none of those are suitable in the context of large scale systems offering one-to-many matching process functionality. There are however other promising pseudonymisation techniques, which are based on partial or complete removal of identity information or the sole use of non-encrypted templates with technical references. These alternative strategies would allow fingerprints to be distributed in a secure way, similar to the protection afforded to the distribution of alphanumeric identity information. These strategies are referred to in the implementation scenarios described under section 6 of this study.

If significant funds were invested in order to try to develop more advanced privacy-protection technology, the European Commission would be a forerunner in this area. Considering the remaining significant technical challenges, it is not a given that such a research project would succeed in a short time, even if significant funds were available. In addition, the need to develop such advanced template protection technique appears to be unique to the ECRIS TCN project and is not a requirement shared with other Commission fingerprints initiatives or a current market need.

[25] 2012 Working Party 29 opinion (WP193), page 31 part 5.4.1 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

4 State of play regarding the use of fingerprints in European systems

This section aims at presenting an analysis of the use of fingerprints in large scale European systems. It presents a number of practical examples of current fingerprint exchange and matching mechanisms in European systems and their approach.

4.1 EURODAC

The EURODAC system is a centralised database of fingerprints to assist with the identification of asylum applicants across Member States. It has been in operation since 2003 and is operated by eu-LISA[26]. There is various information provided in a EURODAC transmission, but the main identifier of the subject is simply a reference number provided by the Member State which collected the fingerprints. Only the Member State which collected the fingerprints holds the link between the reference number and the real subject details (held on their own system at national level). Other personal data on the subject are not exchanged, with the exception that the transmission includes the gender (sex) of the subject – male or female.

Standard fingerprint images are provided (in NIST format) so that the EURODAC system can carry out a feature extraction process using its own technique.

As there is no additional identification data provided about the subject – only fingerprints and a reference number – the fingerprints exchanged are regarded by EURODAC users as being pseudonymous.

4.2 Visa Information System (VIS)

The VIS allows Schengen States[27] to exchange visa application information. It is operationally managed by eu-LISA. It consists of a central IT system and of a communication infrastructure that links this central system to national systems. The VIS connects the central system with consulates in non-EU countries and all external border-crossing points of Schengen Area. It processes data and decisions relating to applications for short-stay visas to visit, or to transit through the Schengen Area. The system is able to perform biometric matching, primarily of fingerprints, for identification and verification purposes.

Ten fingerprints and a digital photograph are collected from persons applying for a visa. This biometric data, along with data provided in the visa application form, is recorded in a secure central database. Fingerprints are retained as images, standard fingerprint templates are used for search purposes and no special template protection techniques are used.

Ten-digit finger scans are not required from children under the age of 12 or from people who physically cannot provide finger scans. Frequent travellers to the Schengen Area do not have to give new finger scans

[26] European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice.
[27] The Schengen States encompasses most EU Member States, except for Bulgaria, Croatia, Cyprus, Ireland, Romania and the United Kingdom. Associated Schengen States such as Iceland, Norway, Switzerland and Liechtenstein are also connected to the VIS. Bulgaria and Romania are currently in the process of joining the Schengen Area.

every time they apply for a new visa. Once finger scans are stored in VIS, they can be re-used for further visa applications over a five-year period.

At the Schengen Area's external borders, the visa holder's finger scans may be compared against those held in the database. A mismatch does not mean that entry will automatically be refused - it will merely lead to further checks on the traveller's identity.

Competent visa authorities may consult the VIS for the purpose of examining applications and decisions related thereto.

The authorities responsible for carrying out checks at external borders and within the national territories have access to search the VIS for the purpose of verifying the identity of the person, the authenticity of the visa or whether the person meets the requirements for entering, staying in or residing within the national territories.

Asylum authorities only have access to search the VIS for the purpose of determining the EU State responsible for the examination of an asylum application.

In specific cases, national authorities and Europol may request access to data entered into the VIS for the purposes of preventing, detecting and investigating terrorist and criminal offences. Data is kept in the VIS for five years.

4.3 Schengen Information System (SIS)

The Schengen Information System (SIS) is a highly efficient large-scale information system that supports external border control and law enforcement cooperation in the Schengen States[28]. The main purpose of the SIS is to help preserving internal security in the Schengen States in the absence of internal border checks.

The second generation Schengen Information System (SIS II) started operation in April 2013.

SIS II enables competent authorities, such as police and border guards, to enter and consult alerts on certain categories of wanted or missing persons and objects. For alerts on persons the minimum data-set is name, gender, a reference to the decision giving rise to the alert, and the action to be taken. In addition, when available, photographs and fingerprints must be added.

SIS II provides the possibility to store and process fingerprints in order to confirm the identity of the persons located as a result of an alphanumeric search. In addition, the inclusion of an Automated Fingerprint Identification System (AFIS) in SIS II in the future will allow the identification of persons on the basis of their fingerprints. An efficient SIS AFIS function has been identified as an opportunity for improving security. It is understood[29] that the intention is to have a 'central' AFIS operational during 2017. It is foreseen that Member States would then have the option of when they connect and start using it.

[28] The Schengen Area encompasses most EU Member States, except for Bulgaria, Croatia, Cyprus, Ireland, Romania and the United Kingdom. The 22 EU Member States that are part of the Schengen Area fully operate the SIS. Four Associated Countries that are part of the Schengen Area (Switzerland, Norway, Liechtenstein and Iceland) fully operate the SIS. Special conditions exist for EU Member States that are not part of the Schengen Area (Bulgaria, Croatia, Cyprus, Ireland, Romania and the United Kingdom).

[29] Notes from SIS II meeting in Brussels on 17 March 2016.

In the SIS context, although Member States are already attaching fingerprints to alerts, the quality is variable, which impacts on the usability. The first step for the new AFIS project is to create and implement a standard for the NIST metadata associated with each fingerprint image provided for exchange / filing.

According to eu-LISA the implementation of an AFIS used in SIS is estimated at EUR 9,500,000 for development and EUR 1,200,000 yearly recurring operating costs.

4.4 Prüm arrangements

Prüm provides a decentralised mechanism, available to many Member States, for the exchange of fingerprints for law enforcement purposes. Currently there are 21 Member States who are using the Prüm network in respect of fingerprints. Not all these are fully operational with all other operational Member States and in a handful of cases, a single Member State may only be connected to very few other Member States.

The work by the Prüm community and particularly the DAPIX Group (Working Party on Information Exchange and Data Protection), concluded, in relation to the Prüm exchange, as cited in COUNCIL DECISION 2008/615/JHA of 23 June 2008, the following in regards to data protection[30]:

> *"The hit/no hit system provides for a structure of comparing anonymous profiles, where additional personal data is exchanged only after a hit, the supply and receipt of which is governed by national law, including the legal assistance rules. This set-up guarantees an adequate system of data protection, it being understood that the supply of personal data to another Member State requires an adequate level of data protection on the part of the receiving Member States."*

In effect, Prüm satisfies the data protection requirements by applying the pseudonymisation technique of removing identification data from the fingerprints. All that is provided with a set of fingerprints supplied from one Member State to another for search purposes is a simple reference number. The link from this reference number to the identity information on the subject of the fingerprints is only known to the owning Member State.

The Impact Assessment accompanying the proposal for a Directive amending Council Framework Decision 2009/315/JHA, regarding ECRIS and TCN, and replacing Council Decision 2009/316/JHA, has found that existing EU instruments for the exchange of information cannot be utilised for the purpose of ECRIS TCN.

Based on the original Impact Assessment, the Prüm exchange mechanism was ruled out, as it has significant capacity constraints and only covers the exchange of fingerprints and not biographic data. In the Prüm arrangements Member States have agreed quotas with one another, which determine the amount of fingerprints they can search against in their respective AFIS. Owing to the fact that every Prüm fingerprint hit has to be manually verified by the requesting Member State, the daily throughput is often in single figures.

[30] Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

4.5 Interpol AFIS System

Whilst the Interpol AFIS is not an EU system, it was felt that it would be helpful to include some background information as to how the system operates.

The purpose of the Interpol AFIS is to assist in the detection of crime and identification of persons for all Interpol Member States. All EU Member States have access to the database via their Interpol national central bureau but access is not just restricted to the EU countries.

The Interpol AFIS is a central system, which is managed at the Interpol General Secretariat in Lyon, France. All Interpol Member Countries are able to supply fingerprints for uploading or searching against the AFIS.

The Interpol AFIS database is a centralised system with a capacity of 1 million fingerprint sets, tenprints or crime scene marks and is capable of processing 3,000 requests each 24 hours. Interpol manages a database of more than 233,000 fingerprint records (as of October 2015), authorised users in Member State countries are able to view, submit and cross check fingerprint records using I-24/7 Interpol's secure global communications network, via AFIS. Interpol have undertaken to expand the capacity in correlation to usage by member countries. All available personal data can be reported with the hits and upon a hit, all countries involved are informed. Interpol encourages that tenprints of non-nationals are loaded to the database as well as unsolved crime scene marks.

There are well established processes in place for the loading of fingerprint images and biographical data, they are submitted to the Interpol General Secretariat to be uploaded to the database and saved in NIST format.

The Interpol Fingerprint Unit provides a service through an AFIS gateway which allows Member States to submit remotely a fingerprint search (INT-I compliant file) against the Interpol AFIS database with a "Hit", "No Hit" response typically within 10 minutes, personal data is reported in the case of a "Hit".

Interpol Member States (including all EU Member States) acknowledged a draft resolution concerning improving the population of the Interpol forensic databases at the Interpol General Assembly held in Singapore in 2009. This specifically included the request to populate the databases with data of non-national offenders.

5 State of play regarding the use of fingerprints in Member States

A number of research activities have been carried out in order to establish the state of play regarding fingerprints in the 28 Member States. In particular, 5 Member State visits were carried out and "country fiche" documents were compiled for each Member State using secondary research methods (existing literature). These were then sent to all Member States for verification. The country fiches for each Member State are presented in Annex 4.

The results of the Member State visits and the country fiche exercise, which included existing secondary data in some areas, showed that in 25 Member States, fingerprints are managed by the Ministry of Interior (police) and in 3 Member States fingerprints are managed by forensic institutes.

The research identified that 9 Member States include fingerprints in their national identity card registers, 4 Member States include fingerprints in their resident registers and 1 Member State includes fingerprints in its electoral register. Other systems and applications, for which fingerprints were being used, include asylum applications/ immigration, visas and passports.

It is believed that all Member States have a searchable AFIS system, albeit the Unisys report of 2010[32] indicated that one Member State did not have an AFIS system at that point in time. The majority of Member States use a semi-automated one-to-many matching process in one of their AFIS systems. This means that they have set up an automatic hit-no-hit search mechanism, and that if any hits occur, they are then followed up by a human verification process.

All Member States take tenprints in a criminal context. Altogether, 18 Member States take electronic and ink fingerprints, 1 Member State only takes electronic fingerprints, 5 Member States only take ink fingerprints and 4 Member States did not provide information in regards to the taking of fingerprints.

In 18 Member States, criminal records are managed by the Ministry of Justice, whilst in 10 Member States, criminal records are managed by the Ministry of Interior (police). In total, only 7 Member States have a link between their criminal register and their national fingerprint database. In some cases, the link is a reference number. On the contrary, 19 Member States do not have a link between their criminal register and their national fingerprint database, but 4 are considering developing one. Furthermore, 2 Member States did not provide information in regards to a link between the criminal register and the national fingerprint database.

During the Member State visits, it became evident that there are various AFIS vendors and AFIS versions across the EU, which utilise variable matching threshold controls. This means that each Member State utilises different matching thresholds when processing fingerprint requests. A Member State suggested that it would be helpful to carry out an audit of all AFIS systems across the EU in regards to ECRIS TCN, in order to ensure that the matching mechanism is as refined as possible and in order to exercise some form of threshold control.

Most Member States reported that if existing AFIS were to be used in Member States for the purposes of ECRIS TCN exchanges, there would be a requirement to review existing software licence conditions. It was considered that to accommodate the anticipated volume of tenprints searches, AFIS vendors would seek to

increase their annual charges. This has certainly been the experience of a number of Member States in respect of the implementation of the Prüm arrangements.

The ECRIS TCN initiative foresees a fully automated hit/no hit search followed by an ECRIS request to the Member State(s) where a fingerprint hit is identified. Member States considered it would be important to manually verify the identity of a TCN in the case of a hit at some point in the process. An important part of this consideration is that the underlying principle of ECRIS is that the responsibility for identifying a person lies with the 'requested' Member State. Therefore, it would seem prudent that the verification of identity is done in the second stage following the automated hit/no hit process. In recognition of this, some Member States were concerned that there would be an imbalance in the amount of fingerprint work required between them. The Member States who receive a greater number of ECRIS TCN requests, relative to the scale of their infrastructure, would be required to carry out a significant number of verifications as the 'requested' Member State. This resource implication requires careful attention as the solution is further developed.

The visits also showed that there are various capturing processes employed to gather fingerprints implemented by Member States. There are also various levels of quality in regards to fingerprints taken from individuals, which will need to be taken into consideration. The process involves various organisations (e.g. Ministry of Justice, Ministry of Interior, Forensic Institute, etc.) and Member States emphasised that the linking up of the criminal justice process in terms of fingerprints will take a significant amount of time.

5.1 Important considerations on the use of fingerprints for ECRIS TCN exchanges

This section sets out a number of important considerations in regards to the exchange of fingerprints in an ECRIS TCN context, including volume, availability and the capturing quality and matching of fingerprints.

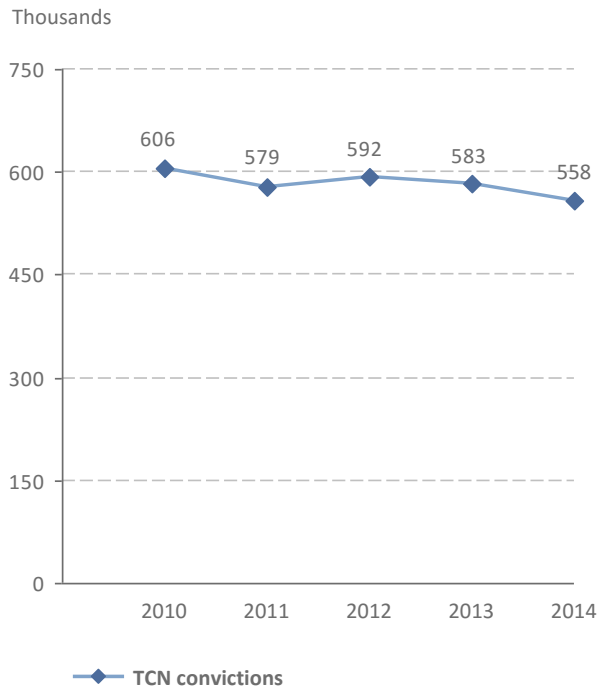
5.1.1 The size of the problem

According to Eurostat information, TCN residing legally in the EU on 1 January 2014 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[31]. The number of TCN residing in the EU is expected to increase in the future.

There have been several statistical surveys, which have looked at the volume of convictions of TCN in the EU. The outcome of the surveys is illustrated in the Figure 2 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.

[31] Analytical Web Note 3/2015, demography report, Eurostat, http://ec.europa.eu/eurostat/documents/7330775/7339482/Demography+report+%E2%80%93+2015+edition/ce8144e3-8e9b-427d-b6a2-61ff42950d41.

Figure 2 Number of TCN convictions per year in the EU (19 Member States)



The impact assessment furthermore explored a number of studies carried out, including the 2010 Unisys study[32] and the KURT SALMON Assessment of ICT impact[33]. This enabled the study to provide an overview of the most recent estimated volume (numbers in thousands of convicted TCN). Table 2 and Figure 3 below illustrate the distribution of the number of TCN convictions across Member States[34].

[32] Feasibility Study: Establishment of a European Index of Convicted Third Country Nationals, Unisys, 2010. Available at: http://ec.europa.eu/justice/criminal/files/tcn_feasibility_final__report_en.pdf.
[33] 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. Available at: http://ec.europa.eu/justice/criminal/files/ecris_tcn_ict_impact_assessment_final_report_en.pdf.
[34] Both the Unisys Feasibility Study and the Kurt Salmon ICT Impact Assessment Study also collected statistics concerning the volume of TCN convictions per Member State.

Table 2 Number of convicted TCN (in thousands) provided through several surveys[35]

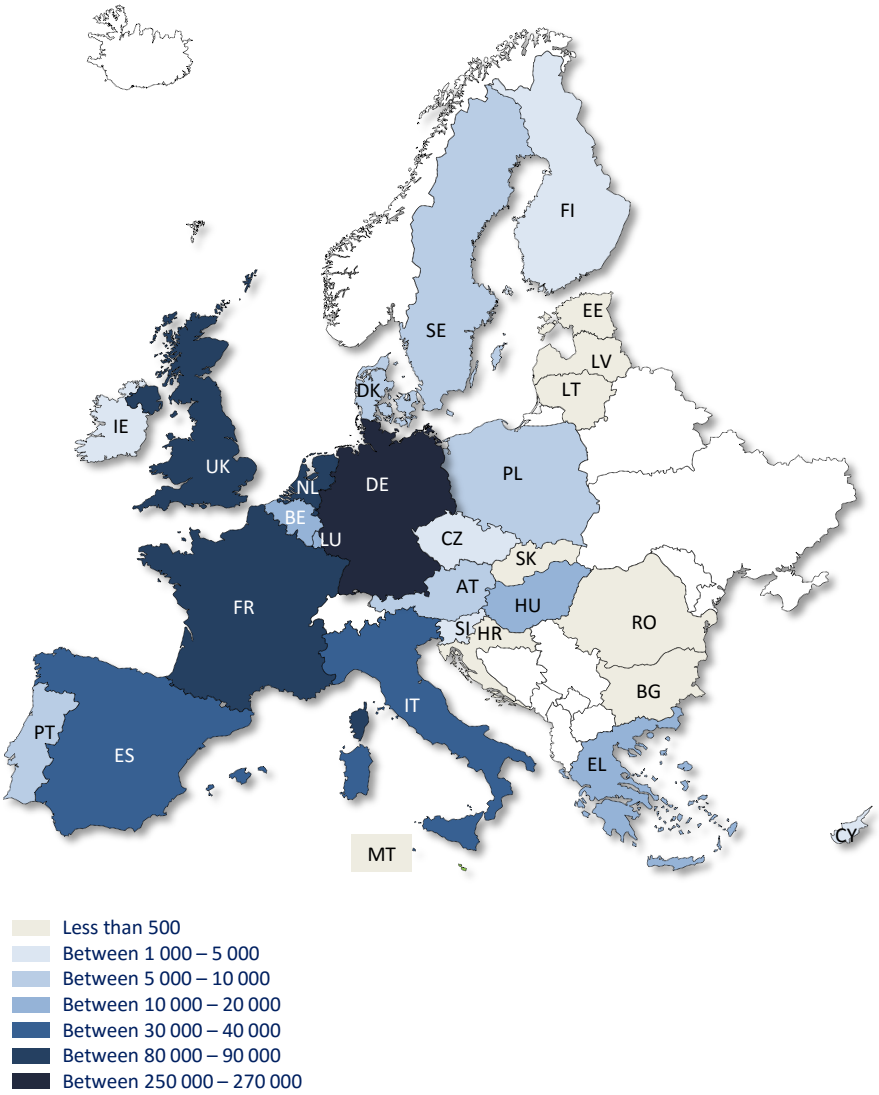
Member States / Surveys	Estimates*	2012	2014	2015
Austria			44.4	
Belgium				304.5
Bulgaria	61*			
Croatia				2.7
Cyprus		21		
Czech Republic		18		
Denmark	44.7*			
Estonia		2.5		
Finland			6.9	
France		714.7		
Germany				817.2
Greece				598.4
Hungary			9.3	
Ireland	52.9*			
Italy				971
Latvia				94.9
Lithuania			3	
Luxembourg				9.1
Malta	1			
Netherlands				534
Poland				30.3
Portugal				42.7
Romania				0.03
Slovakia	2.3*			
Slovenia		5		
Spain				790.8
Sweden				73.8
United Kingdom	500*			
Total	**661.9**	**761.2**	**63.6**	**5,756.2**

*Where data was not submitted, estimates were calculated on the basis of Member State TCN population (BG, DK, IE, SK and UK).

As confirmed by statistical surveys carried out between 2012 and 2015, it is reasonable to assume that there were at least 6 million convicted TCN in the EU in 2014.

[35] 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, p. 22 of the annex.

Figure 3 Number of TCN convictions in the EU in 2014[36]



5.1.2 Availability and access to fingerprints

The Impact Assessment accompanying the proposal for a Directive amending Council Framework Decision 2009/315/JHA, regarding ECRIS and TCN, and replacing Council Decision 2009/316/JHA, clearly states that:

> *"Many Member States do currently not use fingerprints in their national criminal record registers or are connected to their national AFIS. Likewise, some Member States are concerned about possible double standards for EU nationals on the one hand and TCN on the other hand and the fact that not all convicted persons contained in the national*

[36] 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), p.20, Kurt Salmon, Brussels, 4 December 2015. Available at: http://ec.europa.eu/justice/criminal/files/ecris_tcn_ict_impact_assessment_final_report_en.pdf

criminal record registers have had fingerprints taken, as national rules differ according to categories of offences and between Member States."

This is also confirmed by the findings of the Unisys feasibility study on the establishment of a European index of convicted TCN[37]. The document states that whilst Member States make use of their national AFIS systems, most of them are operated by police authorities and ministries of interior. In the majority of Member States, the ministries of interior hold exclusive access rights to AFIS.

Table 3 Authorities with access to the national AFIS system[37]

Authority with access to AFIS	Percentage of MS
Police	100%
Courts	8%
Central Authority managing CR	8%
Other	23%

The Unisys feasibility study[37] highlights that the above table implies that the authority managing fingerprints should be placed within the police structure. However, some Member States' experts have indicated that they would opt for the development of a new fingerprint database within the Ministry of Justice/Central Authority (if different) in case fingerprints were used in the context of criminal record information exchange.

"The storage of fingerprints in the different national databases is also linked to the stage within the criminal justice chain in which fingerprints are captured. Some of the Member States either have fingerprints information available in their Criminal Records Register or have established a link between the Criminal Records Register and a national AFIS. This is not the case in most Member States however. If fingerprints are to be exchanged in support of the criminal record exchange for third country nationals, the two databases will therefore have to be linked by a unique identifier in order to store and exchange fingerprints data at transnational level."

5.1.3 Capturing of fingerprints

The Unisys feasibility study[37] established that only one third of the Member States were confident that 100% of their convicted persons were being fingerprinted and that for some Member States, there were limitations in regards to the seriousness of the offence, or the length of the sanction imposed in regards to the offence.

On 21 March 2016, the EU Presidency (the Netherlands) reported to the Working Party on Judicial Cooperation in Criminal Matters (COPEN) on the findings of a survey they launched to all Member States, regarding their national use of fingerprints. The findings indicate that fingerprints are taken at different stages of the criminal justice process by different agencies across Member States. Fingerprints are taken from suspected, charged and/or convicted persons. Some Member States indicate that fingerprints are not taken

[37] Feasibility Study: Establishment of a European Index of Convicted Third Country Nationals, Unisys, 2010. Available at: http://ec.europa.eu/justice/criminal/files/tcn_feasibility_final__report_en.pdf.

in all cases and that a range of factors influence whether fingerprints are taken. These include the seriousness of the offence and whether the individual has previously been fingerprinted at an earlier part of the criminal justice process for example. This survey has identified that the police generally capture fingerprints from suspected/arrested persons whilst the courts, in some Member States, capture the fingerprints of those convicted.

5.1.4 Quality of fingerprints

The Unisys feasibility study on the establishment of a European index of convicted TCN rightly highlights the issue of the varying levels of quality in regards to fingerprints held by Member States in AFIS systems[38]:

> *The quality of data is a critical factor for the efficiency of an AFIS. In some other large-scale IT systems, such as VIS, data capture and storage takes place in real-time. This is not the case for ECRIS TCN: at the present, the exchange of fingerprints for identification purposes is undefined. This leads to a conclusion that the quality of the prints should be checked at the source during the enrolment and/or after the system has proposed a number of hits.*
>
> *There are significant differences in the way Member States perform the fingerprint capture. Moreover, various fingerprint quality thresholds apply due to the different techniques used. Therefore, quality standards (e.g. use of Livescans), guidelines and procedures to optimise quality should be used in the case of the Central Index. With regard to a decentralised solution, each Member State will be responsible for defining fingerprint quality thresholds based on results matching and statistics thereof.*

5.1.5 Matching of fingerprints

It is estimated that around 700,000 convictions are registered in regards to TCN each year within the EU, where fingerprints could be taken and stored under the new legislative proposal[39]. This being the case, even if no previous TCN records were used for ECRIS TCN exchanges and a “day one forward” approach was adopted, within a year the size of the ECRIS TCN collection would be larger than the national AFIS systems operated in most of the Member States. The chart below, which is taken from an ECRIS Fingerprint Exchange Network report[40] from 2014, illustrates this point:

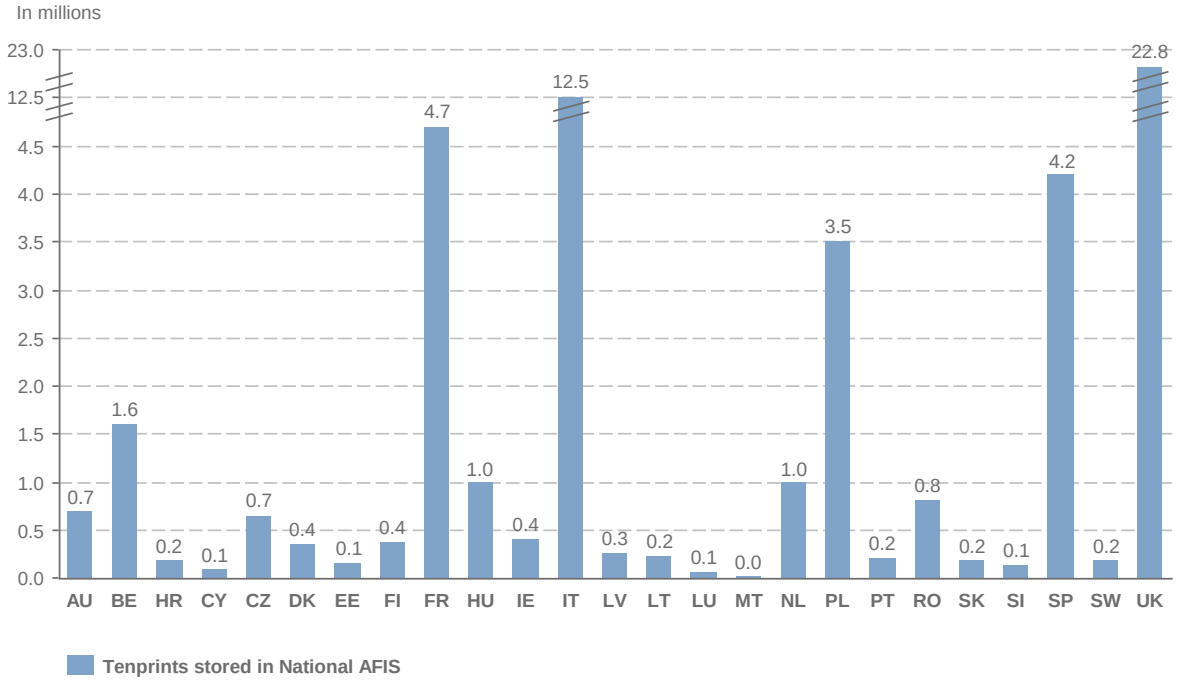
---

[38] Feasibility Study: Establishment of a European Index of Convicted Third Country Nationals, Unisys, 2010. Available at: http://ec.europa.eu/justice/criminal/files/tcn_feasibility_final__report_en.pdf

[39] 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), p.19, Kurt Salmon, Brussels, 4 December 2015. Available at: http://ec.europa.eu/justice/criminal/files/ecris_tcn_ict_impact_assessment_final_report_en.pdf

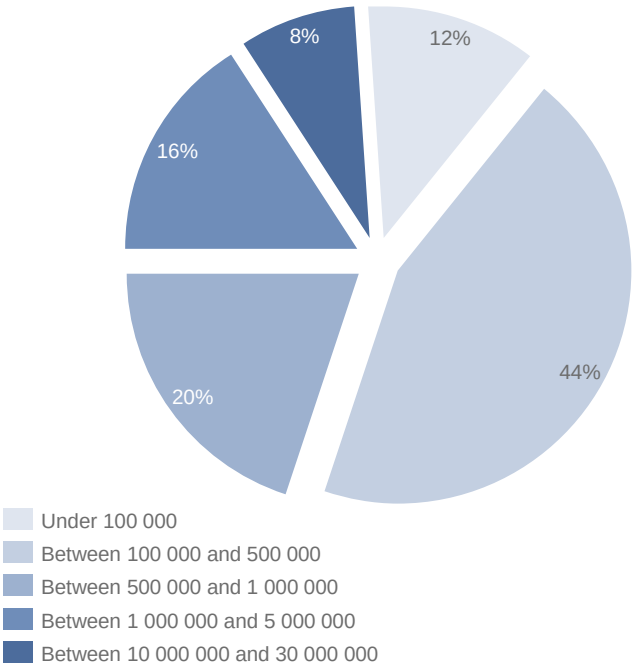
[40] Analysis on the use of Fingerprints within EU Criminal Record Exchange, EFEN (ECRIS Fingerprint Exchange Network) Project work stream one, 2014

Figure 4 Number of tenprints stored in National AFIS as of 2014



Whilst the precise figures may have altered slightly since the original report, the general scale is expected to have remained the same. Of the Member States surveyed, 16 have a national database of less than 700,000 records and 5 Member states have a database of between 800,000 and 4 million fingerprint records. 4 Member states have a database of over 4 million records, with Italy and the UK having considerably larger fingerprint databases than other Member States.

Figure 5 Percentage breakdown of number of tenprints held in national AFIS systems



It can therefore be appreciated that if one of the proposed scenarios is chosen, where each Member State is provided with a copy of the entire ECRIS TCN fingerprint database (a fully distributed approach), this would have a significant practical impact on many Member States. It would be impossible for many national AFIS systems to meet the substantial increase in the number of tenprints that needs to be stored, which would necessitate a complete replacement of the national AFIS.

Conversely, if one of the proposed options is chosen whereby each Member State is only responsible for managing their own locally captured TCN fingerprints and making these available for search by other Member States – in a decentralised approach – the impact on database change and scalability is significantly reduced. Consideration must be given to the cost, scale and deliverability of a distributed fingerprint matching solution that contains the entire TCN database from all Member States, against a centralised or decentralised option where each Member State maintains its own set of TCN fingerprints.

The ongoing growth of an ECRIS TCN fingerprint database will naturally depend on the numbers of TCN convicted and fingerprinted, as well as on legal and/or policy decisions considering retention time limits for these fingerprints within the database. Assuming that numbers continued to grow at 700,000 per year, and that retention was set to be in excess of ten years, within five years the database would have grown to 3.5 million fingerprints and within ten years to 7 million fingerprints. The impact of this scale is, further to the statements above, of considerable implication to the AFIS solutions provided in Member States to deal with it. In particular, searching in this size of database has implications on the appropriate technical approach.

All biometric matching systems have to deal with a level of error rates. In large-scale AFIS solutions, providing one-to-many search functionality, preventing incorrect identifications (the False Positive Identification Rate [FPIR]) and reducing misses (the False Negative Identification Rate [FNIR]) will be crucial in order to deliver the required benefits and meet the solution's business goals. In ECRIS TCN, considering the estimated amount of TCN convictions from across the EU, it is estimated that Member States will need to be able to perform a significant number of "hit/no hit" queries per day. Where reliable fingerprint search responses are required, for example as part of an initial automated "hit/no hit" process, the provision of a highly accurate AFIS with low FPIR and FNIR rates is crucial. The actual number of searches that will require manual verification will ultimately be dependent on where matching thresholds are set.

If an AFIS is scaled at the size required to support an ECRIS TCN fingerprint database, and if very low matching error rates are not maintained, then the system will miss an unacceptably high number of potential matches, which could have serious security implications. Furthermore, the system would generate an unworkable number of incorrect matches, which will lead to an unviable level of manual intervention required to provide resolution.

Therefore, one of the **most important considerations for an effective use of fingerprints within an ECRIS TCN solution is the need for the capture of good quality fingerprints and matching at a high level of accuracy**. A decision has yet to be made on the precise accuracy requirements that are expected to be met or what will be achievable realistically with the available data set. Further work will be required on this subject at a subsequent stage of the ECRIS TCN project. However, for now it is worth noting that in comparable sized AFIS systems with similar business goals, the use of proprietary matching techniques from one of the leading AFIS vendors, would be considered necessary to meet the matching accuracy requirements.

It is not possible to provide a comparison of one-to-many accuracy rates, using standard (unprotected) fingerprint templates from one of the leading AFIS vendors against one-to-many accuracy rates, using a template protection technology approach, as the data is simply not available. To provide a workable one-to-many identification searching solution at the scale and accuracy needed to meet the expected requirements of the ECRIS TCN fingerprint project, the use of operationally proven and tested proprietary fingerprint matching techniques working with standard fingerprint templates is currently the only viable option.

Another important consideration is the **ability to deal with and process potentially poor quality**[41] prints from some subjects (who have inherently poor friction ridge detail), as well as the need for a solution that could support interoperability and would be able to work with existing law enforcement fingerprint capture mechanisms and processes. However, in the context of ECRIS TCN exchanges, Member States should consider having dedicated staff for taking fingerprints, which will drive up the quality of the fingerprints obtained.

Template protection technologies can have difficulties dealing with low quality fingerprint samples. In most cases, these solutions also require a capture process where multiple samples are recorded and stored from the same finger. This is not compatible with existing fingerprint recording procedures in the criminal justice system, where TCN fingerprints are captured using a conventional process of recording ten fingers, either via "Livescan" units (electronic fingerprint capture devices) or through the traditional "ink and paper" collection. In addition, changing fingerprint capture procedures to require multiple captures of the same finger would have a very significant operational impact – both in terms of the increase in time required to record fingerprints but also in terms of updated operator training and changes to operational processes and equipment. These are further significant constraints in regards to the potential deployment of template protection technologies.

It will be important to consider **how fingerprints are taken in order to satisfy the ECRIS TCN requirement**. For example, a number of Member States capture "rolled" fingerprints in order to populate their national AFIS. Rolled fingerprints, by their nature, can introduce a level of variability between different capture sessions due to the extent of the side to side roll undertaken (peripheral friction ridge detail will be missed if the finger is not fully rolled) and the natural elasticity of the skin.

Considering the volume in regards to the ECRIS TCN scenario, automation would need to be considered as much as possible. This can, however, only be achieved effectively, if the fingerprints are of a good quality. Member States would need to comply with a minimum quality standard of fingerprints. As indicated in the Unisys study, all MSs already capture flat tenprints with a resolution of 500 ppi. This in itself is not sufficient, as these could be high-resolution files of a blurred image. Member States would need to ensure that they implement good enrolment conditions, as well as the necessary digital equipment (live-scans) and processes to ensure that the minimum required level of quality is met.

---

[41] There is not a standard, universal threshold that can be set to determine if a fingerprint is "poor quality" and the setting applied in an AFIS context will depend on a set of factors, including whether the solution will reject fingerprints that are deemed poor quality or whether it will attempt to search any fingerprints received, as long as they are capable of being templated. At this stage the measurement and determination of what will be classed as poor quality in the ECRIS TCN fingerprint solution has not been set. Consequently it is not currently possible to give an exact percentage of poor quality fingerprints there will be. However, by way of an example the EURODAC system, which has a fairly strict approach to measurement of fingerprint quality, rejected around 4.5% of fingerprints received during 2014.

6 Technical scenarios

This section details the technical scenarios assessed in this study. It presents the overall rationale for the selection of the technical scenarios and further details each of the technical scenarios that are assessed as feasible for supporting ECRIS TCN exchanges.

Several options were initially identified to implement an ECRIS TCN system such as a decentralised system with a “hit/no hit” function, a decentralised system with a Member State of Reference, a fully-fledged central identification database and a central system with a “hit/not hit” function. Those options were discussed with representatives of the Member States during the ECRIS Expert Group meeting held in September 2014.

Out of those options, four possible scenarios were identified as the most realistic and feasible regarding the exchange of convictions for TCN. Depending on the scenario, it would require the establishment of one or several systems holding identification data of convicted TCN in line with the following considerations:

- The ECRIS TCN system contains alphanumeric identity data of convicted TCN, extracted from the national criminal records registers of the Member States. In the case when information on a particular TCN needs to be obtained, the requesting Member State is able to search the ECRIS TCN system by introducing identity data of the person into the search engine.
- The ECRIS TCN system contains fingerprints of convicted TCN. In the light of the conclusions reached on pseudonymisation techniques, implementation of fingerprint identification functionality in the context of those options is technically feasible. As concluded in earlier sections of this study, the most advanced encryption techniques cannot be applied to fingerprints as all the scenarios identified rely on *one-to-many* matching operations. Pseudonymisation in this context can only be implemented by removing identity data from the fingerprint files.
- Depending on the option, the unique or several ECRIS TCN systems can be searched locally or remotely to find the past criminal history of a particular TCN. Given the anticipated high volumes, the search process needs to be fully automated and produces a “hit” or “no-hit” reply.
- A “hit” provides immediate information on i) whether the TCN concerned has already been convicted in another Member State and ii) which Member State(s) to address for information on these convictions.
- “Hits” on alphanumeric information or fingerprints can only be obtained for TCN identification data that has been uploaded beforehand in the ECRIS TCN systems by the respective Member States..

Regarding the possible implementation choices listed above, the options have thus been further detailed into a set of four technical scenarios as follows:

- Decentralised ECRIS TCN system:
    - Scenario 1: sharing of fingerprints of TCN convicted at national level with all other EU Member States;
    - Scenario 2: no sharing of fingerprints of TCN convicted at national level.
    - For supporting the storage and searching of fingerprints, each decentralised scenario has two variants that each Member State can consider at national level:
        - Variant A: it uses a specific dedicated AFIS which is included in the ECRIS TCN system, or

        - Variant B: it extends and reuses an existing national AFIS and links it to the ECRIS TCN system.
- Centralised ECRIS TCN system:
    - Scenario 3: centralisation of TCN fingerprints only;
    - Scenario 4: centralisation of all TCN identity information (fingerprints and alphanumeric identity information).
    - In both centralised scenarios, storage and search of fingerprints are handled by the central ECRIS TCN system. However the practical implementation of both scenarios still requires the Member States to store and process locally the fingerprints of the TCN convicted at national level (before transmitting them to the central TCN system and also for being able to perform verification of the fingerprints at national level when replying to ECRIS requests). Each central scenario has thus also two variants that each Member State can consider at national level:
        - Variant A: it does not use a dedicated AFIS but relies instead on a simplified storage and processing component for fingerprints, which is embedded in the ECRIS TCN system, or
        - Variant B: it extends and reuses an existing national AFIS and links it to the ECRIS TCN system.

It must be noted here that for the implementation of the ECRIS TCN system, only one of the four technical scenarios can be chosen at EU level. However, within each scenario Member States may opt individually for variant A or variant B depending on their national constraints and preferences. In other words, variants A and B are interoperable within a given scenario.

The specificities of each technical scenario as initially defined in the scope of this study are further described in sections 6.1, 6.2, 6.3 and 6.4 below.

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, in the scenarios it is considered that the CA also operates the national criminal records register. The CA operates the following systems:
    - The national criminal records register stores the information on convictions; this 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 ECRIS TCN system providing features for storing, processing and handling TCN alphanumeric identity information and fingerprints. The ECRIS TCN system is technically integrated and communicating with ECRIS. Depending on the scenarios and variants, the internal components and features of the ECRIS TCN system vary.
- **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.

In addition, the following operational and technical considerations are considered as important and apply to all scenarios presented:

- **How and when the fingerprints of the TCN are enrolled is kept out of scope of this assessment and is left at the discretion of each Member State. For the purpose of this cost estimation, the ECRIS TCN system receives as input a fingerprint file that is compliant with the ANSI NIST standard.**
- **Furthermore it can be safely assumed that this NIST file contains a set of 10 finger images and associated slap (plain) images in WSQ file format. The images have a resolution of at least 500 ppi and have been taken under controlled conditions. They can be considered as being of good quality and suitable for automated matching.**
- **In all scenarios *one-to-many matching* is performed when making the "hit/no hit" searches using fingerprints. Considering the high amounts of such queries that will need to be executed per day, this process needs to be performed fully automatically, without any human verification of the results at this stage. This is considered as acceptable because this process only aims at finding a list of Member States to which further ECRIS requests can be sent. Proper identification and human verifications are to be performed later by the Member States that need to respond to the ECRIS request.**
- **Because of the full automation required for the "hit/no hit" search, the matching accuracy needs however to be optimised in order to avoid as much as possible false-positive and false-negative results. This is to avoid missing possibly known conviction data but also avoid preparing and sending ECRIS requests to Member States that do not have information on a given TCN subject. This study recognizes the need to carefully tune/optimise the AFIS threshold values in order to reach a good balance on false-negative and false-positive results.**

6.1 Description of Scenario 1: decentralised ECRIS TCN system, sharing of fingerprints and local "hit/no hit" search

Scenario 1 is based on the implementation of a **decentralised ECRIS TCN system** with the following key characteristics:

- Alphanumeric identity information of TCN convicted at national level is pseudonymised and systematically shared with all other Member States for storage in their national ECRIS TCN system.
- **Fingerprints of TCN** convicted at national level **are systematically shared** (without further identity information) with all other Member States for storage in their national ECRIS TCN system or AFIS system.
- A Member State searching for the past criminal history of a TCN performs a **local "hit/no hit" search** in its own ECRIS TCN system for identifying which other Member State(s) can be queried for information on these past convictions.

When a TCN is convicted in a Member State, the alphanumeric identity information and the fingerprints of the TCN are stored by the Central Authority in the ECRIS TCN system. The identity information and

fingerprints are pseudonymised before being distributed to all other Member States. As a result, the ECRIS TCN system of all 28 Member States contains the same data, namely the pseudonymised identity and fingerprints of all TCN that have been stored in the criminal record register of any Member State.

In case of a request for past convictions for a TCN, the requesting Central Authority would first search locally in its own ECRIS TCN system. The search result would provide information on i) whether the person concerned has already been convicted in another Member State and ii) which Member State to query for information on this conviction. In case of a "hit", in a second step, the requesting Member State would contact directly the Member State identified as holding the conviction information using ECRIS.

6.1.1 Description of Scenario 1A

The following sections provide an overview of Scenario 1A and detail the main business processes regarding the exchange of information.

6.1.1.1 Overview

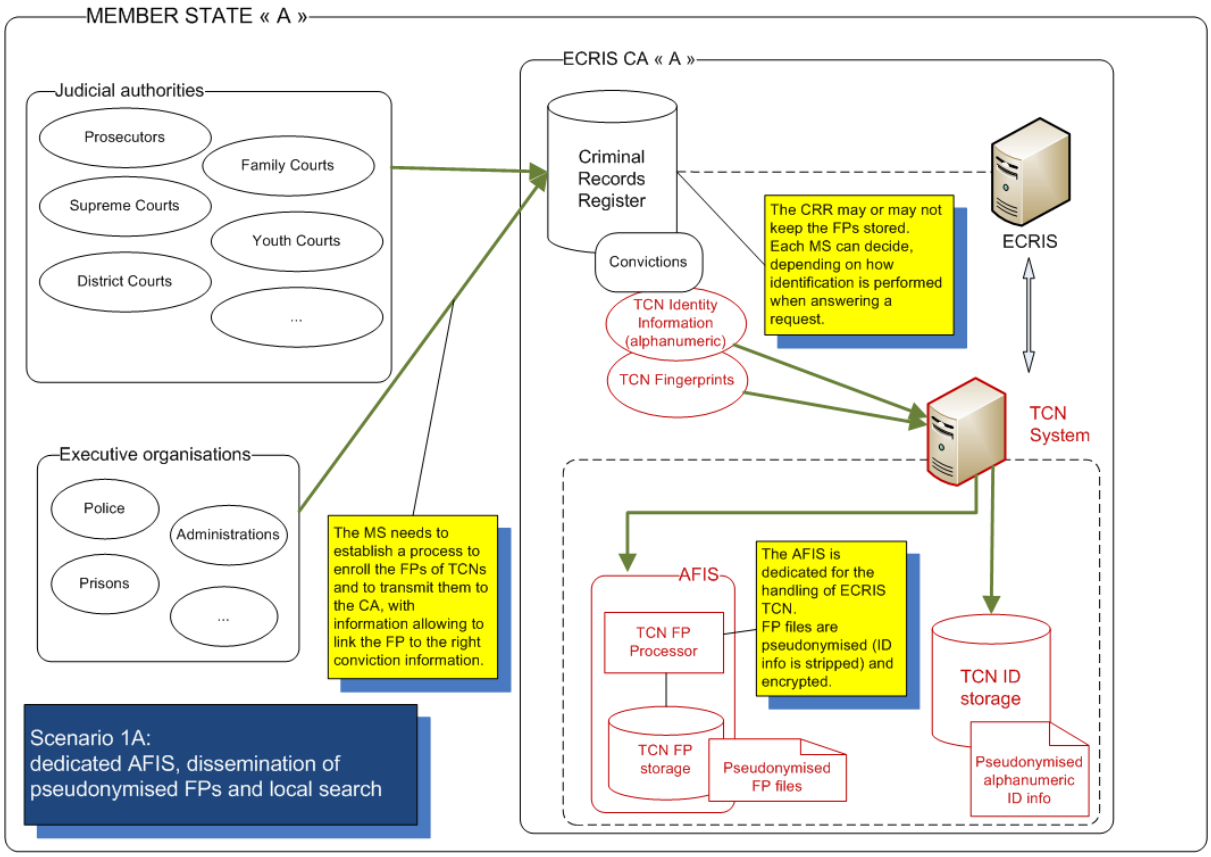
In Scenario 1A, the Member State does not rely on an existing national AFIS. Instead, the ECRIS TCN system at national level needs to include a dedicated AFIS for the purpose of handling the TCN fingerprints.

In Scenario 1A the ECRIS TCN system is composed of:

- A dedicated AFIS which is composed of a server capable of processing fingerprint files, of storing these fingerprints internally and of performing one-to-many matching;
- A TCN ID storage for processing, storing and matching alphanumeric identity information.

It is important to note that the 2 components are completely separated and isolated in such a way that it is not possible to link the fingerprints kept in the AFIS to any identity information kept in the TCN ID storage. Both fingerprints and alphanumeric identity information are pseudonymised for protecting as much as possible the personal data. Figure 6 illustrates the overview of Scenario 1A.

Figure 6 Overview of Scenario 1A



6.1.1.2 Process: new conviction of a TCN

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.

(3) The CA first stores the conviction information and alphanumeric identity of the TCN in the national criminal records register. It may also keep the fingerprints but this is not strictly necessary.

Then the CA enters the data into the ECRIS TCN system, the identity information and fingerprints. In addition the CA may also provide a unique technical reference to the ECRIS TCN system. This reference is known in the national criminal records register and serves in the later processes for finding back the corresponding conviction data.

(4) The ECRIS TCN system performs 2 operations in parallel:

a. It extracts the alphanumeric identity information provided, runs it through a pseudonymisation technique and stores the pseudonymised ID information in the TCN ID storage.

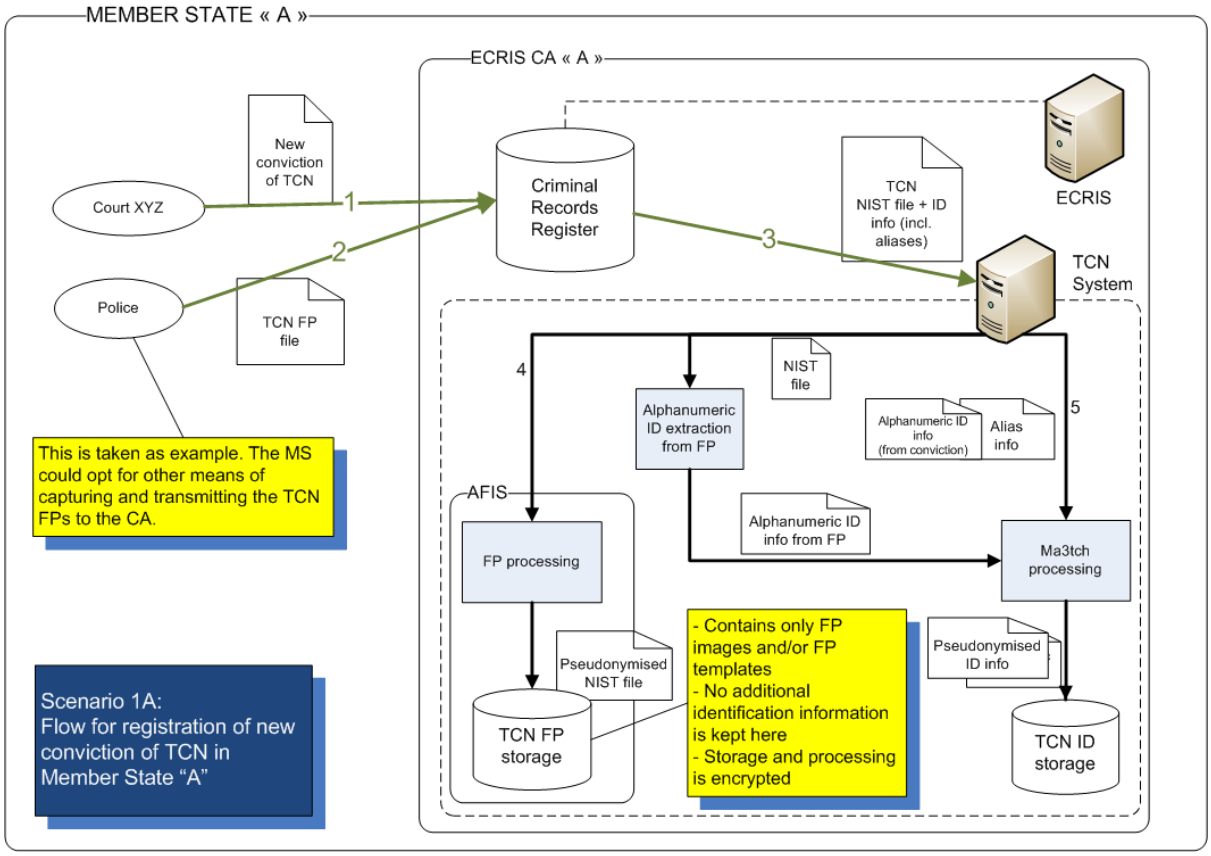
b. In parallel it provides the NIST file as input to the dedicated AFIS.

The dedicated AFIS performs the following processing:

- It pseudonymises the fingerprint file. This is done by removing all alphanumeric information (i.e. the Type 2 data inside the NIST file). More generally, only the tenprints images are extracted and the remaining information is discarded.
- If necessary for optimising the *one-to-many matching*, the AFIS may also create fingerprint templates for this set of fingerprints. Whether this is necessary depends on the specific product selected for implementing the dedicated AFIS.
- It encrypts and stores the tenprints images, the templates (if any) and the technical reference provided by the CA.

Figure 7 illustrates the described process for Scenario 1A.

Figure 7 Process for a new conviction of a TCN in Scenario 1A



6.1.1.3 Process: dissemination of TCN identity information

The process is triggered by the 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 be triggered systematically whenever new data is entered into the ECRIS TCN system. In this diagram, Member State "A" has convicted a TCN and entered the identity information in its national ECRIS TCN system. "A" now pushes the TCN identity information and fingerprints to all other Member States.

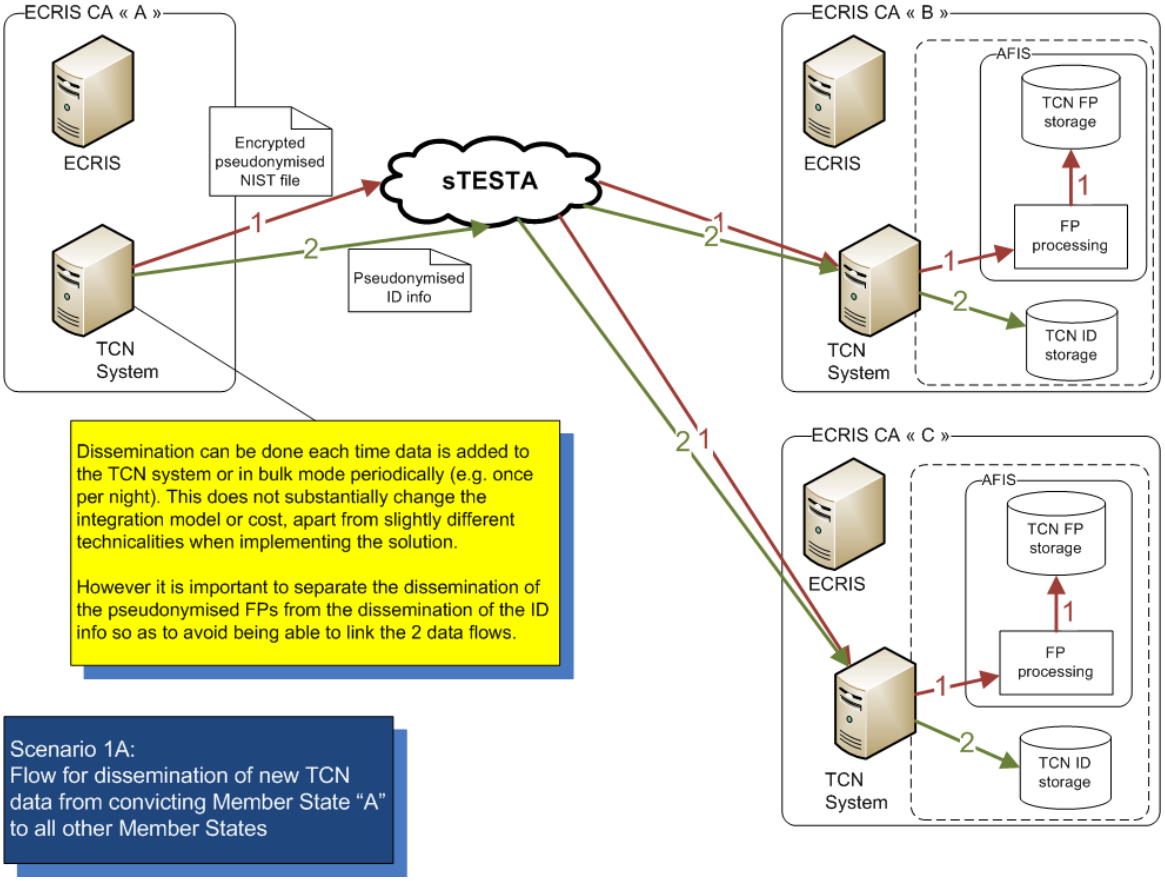
(1) The AFIS in Member State “A” prepares a NIST file that contains only the tenprints fingerprint images and encrypts it. It then sends a message containing this encrypted file and the corresponding national technical reference to all 27 other Member States through the secured sTESTA network (via HTTPS protocol).

The ECRIS TCN system of each Member State receives the encrypted file and passes it on to its embedded AFIS. The AFIS decrypts the NIST file, extracts the tenprints images, and creates the necessary templates. It then encrypts the data and stores all the information in its own database (including the unique technical reference provided by the sender).

(2) In a separate process the ECRIS TCN system of Member State “A” sends the pseudonymised alphanumeric identity information to the 27 Member States. Each Member State stores this information in its local TCN ID storage. This part is handled by the ECRIS TCN system using *Ma3tch* algorithms.

Figure 8 illustrates the described process for Scenario 1A.

Figure 8 Process for dissemination of TCN identity information in Scenario 1A



It is important to note that dissemination of data to the 27 other AFIS systems needs to be a fully automated process. Additionally, it is important to keep the 2 dissemination flows – the one for pseudonymised fingerprints and the one for pseudonymised alphanumeric identity information – separate so as to avoid creating the possibility at any moment to link the two flows of information. In this manner it is never possible to establish a link between fingerprints and corresponding nominal identity information for the receiving Member States.

6.1.1.4 Process: local "hit/no hit" search for identifying Member States holding conviction data

This process starts when a competent authority within the Member State contacts the CA for requesting information on past convictions for a given TCN. The authority provides to the CA the identity of the TCN as well as the fingerprints.

(1) The CA enters the TCN identity information and/or fingerprints into the ECRIS TCN system in order to perform a "hit/no hit" search. The aim is to find which other Member States possibly have information on this specific TCN.

(2) The ECRIS TCN system first triggers a *one-to-many matching* operation on the dedicated AFIS. As a reminder of what has been stated earlier in this document, it is assumed that the file given as input to the AFIS is compliant with the ANSI NIST standard, that it contains fingerprint images of a resolution of at least 500 ppi and that these images are of good quality.
The AFIS performs the *one-to-many matching* and responds internally to the ECRIS TCN system with a list of hits.

(3) For each "hit" the AFIS provides only the Member State and the unique technical reference associated with the fingerprints that produced the "hit".

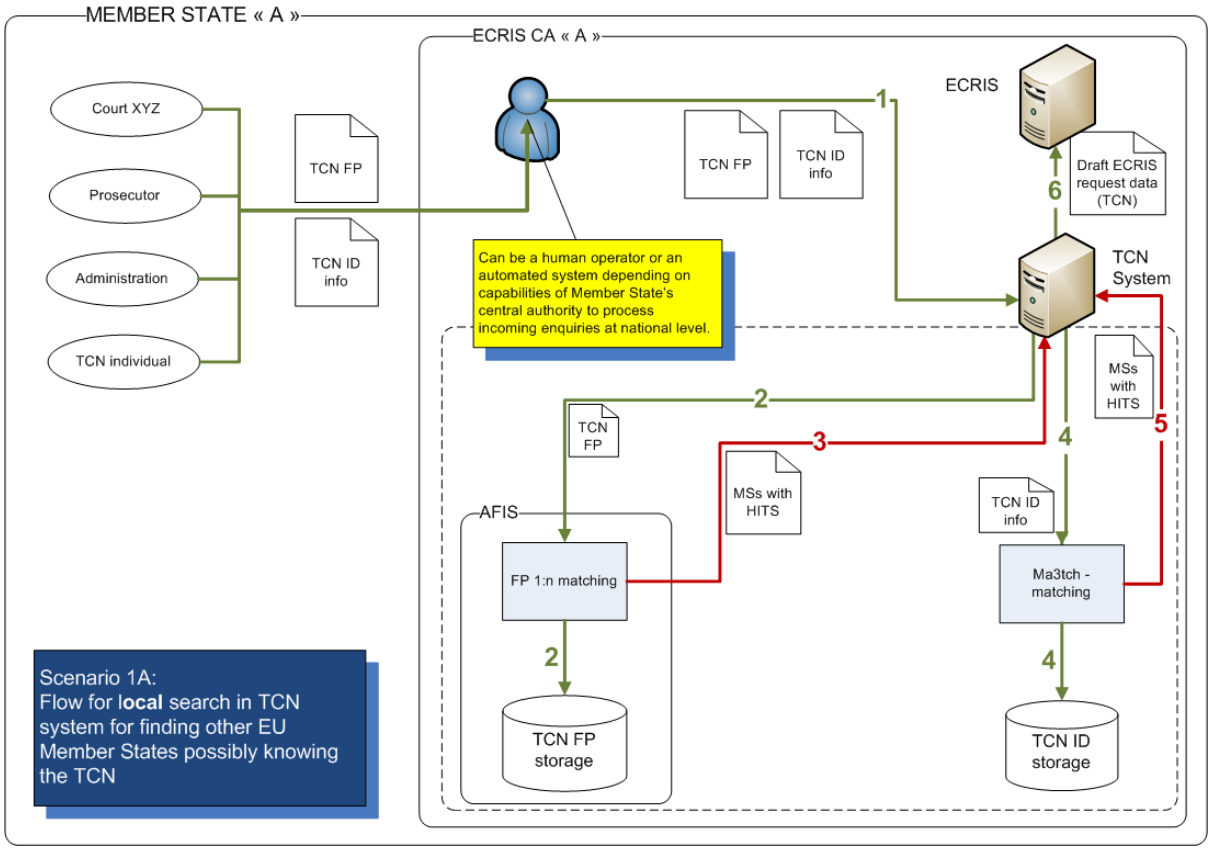
(4) The ECRIS TCN system uses the alphanumeric ID info and performs a matching using the *ma3tch* algorithms.

(5) The *ma3tch* processor returns a list of Member States in which hits have been found.

(6) The ECRIS TCN system consolidates the 2 lists of hits received from the AFIS and from the *ma3tch* processor. It prepares a draft ECRIS request message for each Member State found and inputs these requests into ECRIS.

The ECRIS request that has been prepared contains the alphanumeric identity information, attached NIST file with fingerprints and, when available, the unique technical reference linked to the fingerprint file that produced the "hit". Figure 9 illustrates the described process for Scenario 1A.

Figure 9 Process for local "hit/no hit" search in Scenario 1A



The one-to-many matching is performed fully automatically, without any human verification of the results at this stage. This is considered as acceptable because this process only aims at finding a list of Member States to which further ECRIS requests can be sent. Proper identification and human verifications can be performed later by the Member States that need to respond to the ECRIS request.

The matching accuracy, however, needs to be as high as possible in order to avoid false-positive and false-negative results as much as possible. This is to avoid missing possibly known conviction data but also to avoid preparing and sending ECRIS requests to Member States that do not have information on the given TCN. This study recognises the need to carefully tune the AFIS threshold values so as to reach a good balance on false-negative and false-positive results.

6.1.1.5 Process: ECRIS requests

This process starts after the "hit/no hit" search has been done using the TCN identity information and/or fingerprints. At this moment the ECRIS TCN system has prepared draft ECRIS request messages. In the diagram above, Member State "A" is the requesting Member State and the search has identified 4 other Member States that have information on the given TCN.

(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 4 Member States that were previously identified. Each ECRIS message contains the alphanumeric identification information, an attached NIST file with the fingerprint images where available and (also where available) a unique technical reference associated with the fingerprints that produced the “hit”.

(2) Each Member State receives the ECRIS request message and processes it according to the current mechanisms in ECRIS.

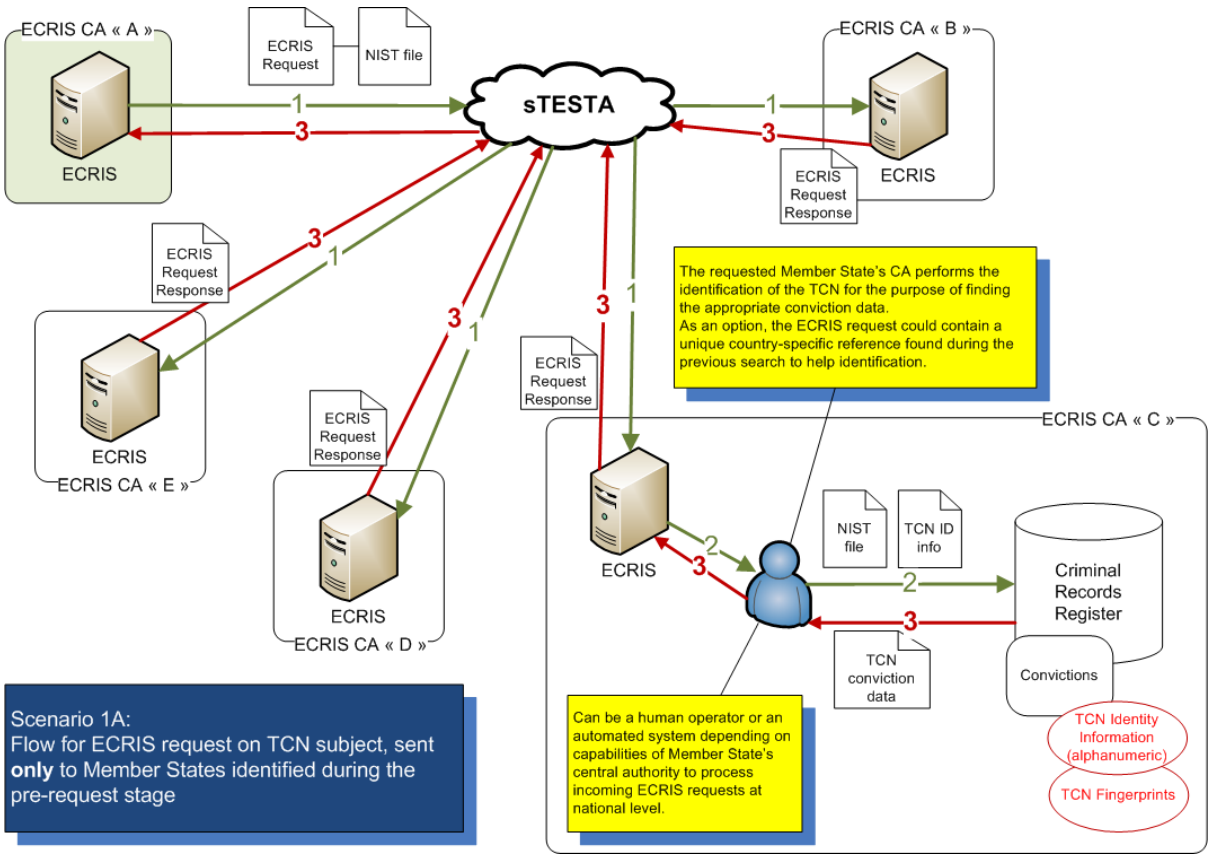
Please note here that in case of doubts on the identity of the TCN the requested CA can use the AFIS embedded in the ECRIS TCN system for performing additional human manual verifications using the fingerprints received with the ECRIS request. In addition, the requested CA may also use other national IT systems available to help in the identification.

(3) 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.

(4) The ECRIS system of the requesting Member State consolidates all the responses received from the 4 requested Member States.

Figure 10 illustrates the described process for Scenario 1A.

Figure 10 Process for ECRIS request in Scenario 1A



6.1.2 Description of Scenario 1B

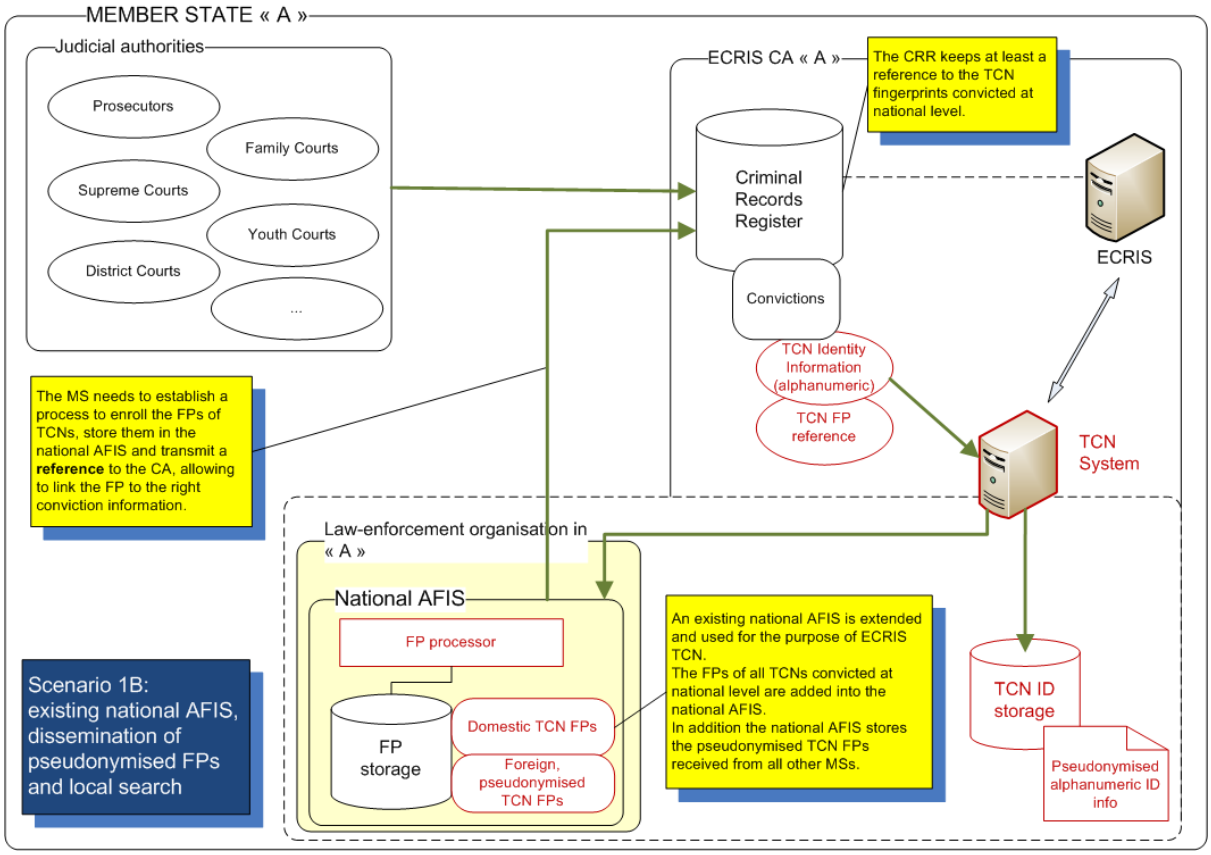
In Scenario 1B, the Member State extends and reuses an existing national AFIS. The ECRIS TCN system at national level does not include a dedicated AFIS for the purpose of handling the TCN fingerprints but links with the national AFIS. It still contains the TCN ID storage and *ma3tch* processing features.

The logic and principles described in detail in the previous section are identical in Scenario 1B. The diagrams below and descriptions highlight mainly the differences between Scenario 1B when compared with Scenario 1A. As also already stated previously, Member States may opt for Scenario 1A or 1B as both are interoperable and can work together in the EU landscape.

6.1.2.1 Overview

The main difference with Scenario 1A is that the ECRIS TCN system does not contain its own dedicated AFIS but links with a national AFIS that is extended and reused for the purpose of handling the TCN fingerprints. The national AFIS is usually typically managed and operated by another organisational body than the central authority handling the criminal records register. The national AFIS needs to be extended in such a way that it can include the fingerprints of TCN convicted at national level (labelled "domestic TCN fingerprints" in the diagram), but also receive and store the pseudonymised fingerprints of TCN convicted by all other EU Member States (labelled "foreign, pseudonymised TCN fingerprints" in the diagram). Figure 11 illustrates the described process for Scenario 1B.

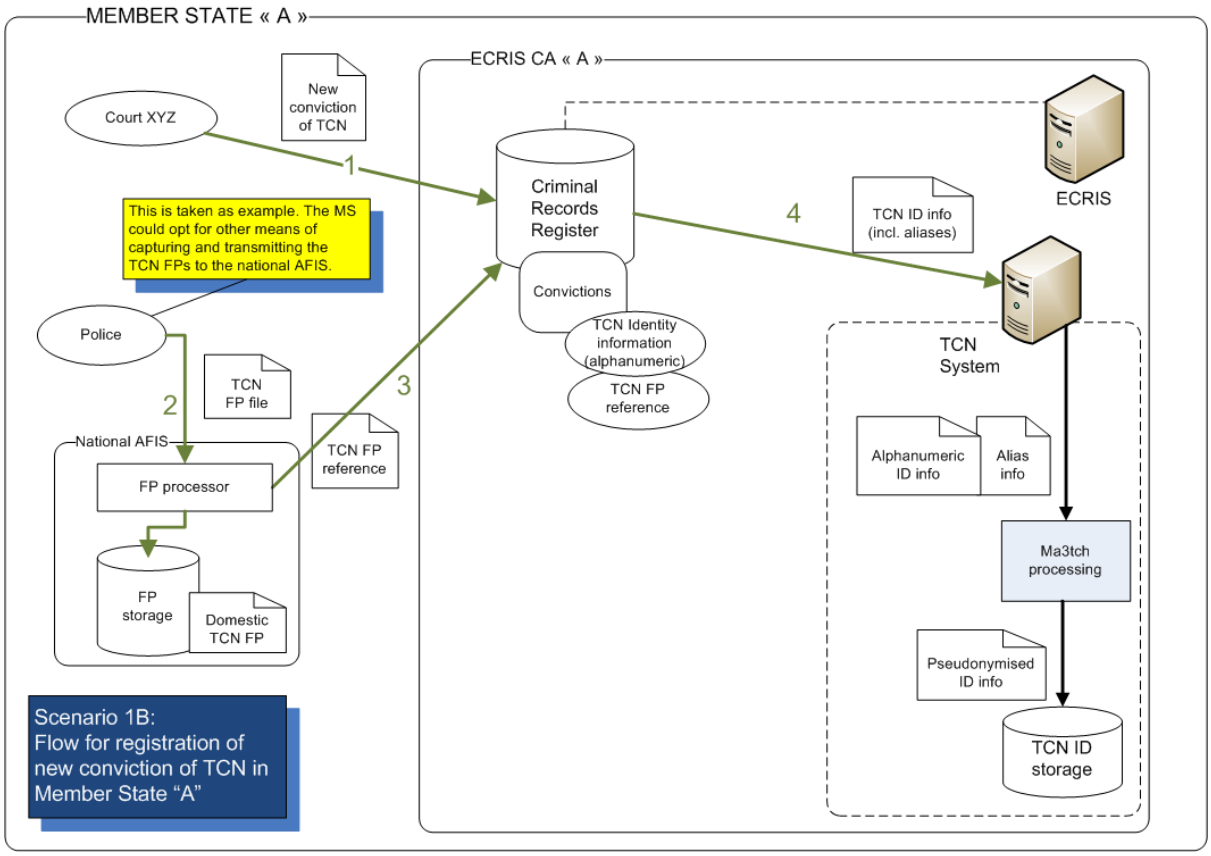
Figure 11 Overview of Scenario 1B



6.1.2.2 Process: new conviction of a TCN

This process is quite similar to the one presented in Scenario 1A, apart from the collection and storage of the fingerprints of the convicted TCN. In this scenario, the fingerprints taken from the convicted TCN are entered into the national AFIS, which then transmits at least a technical reference to the CA. The CA can then link this technical fingerprint reference to the TCN identity and conviction data in the criminal records register. As in Scenario 1A, the CA still feeds the alphanumeric identity information into the ECRIS TCN system which pseudonymises it using *ma3tch* algorithms and stores it in the TCN ID storage. Figure 12 illustrates the described process for Scenario 1B.

Figure 12 Process for new conviction of a TCN in Scenario 1B



6.1.2.3 Process: dissemination of TCN identity information

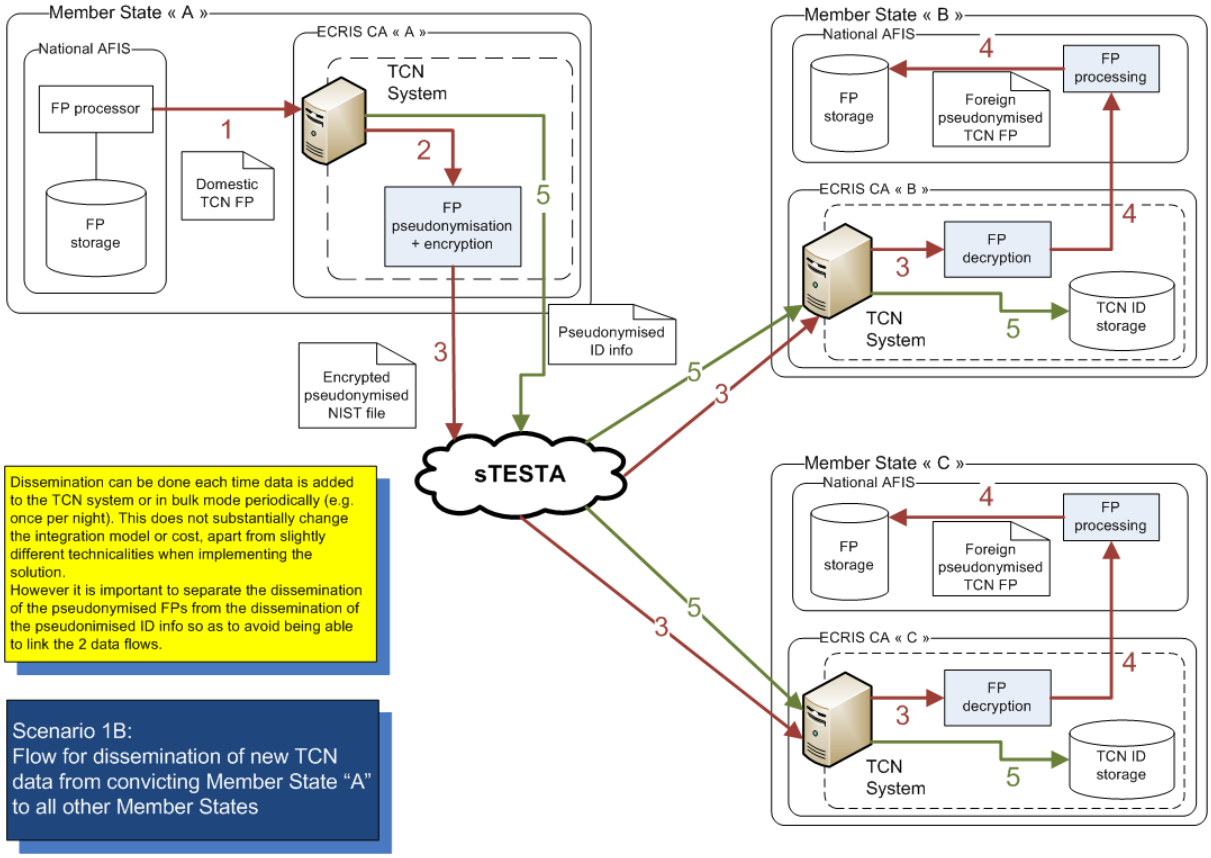
The dissemination of TCN alphanumeric identity information and pseudonymised fingerprints is similar to Scenario 1A. The main differences for Member States opting for Scenario 1B concern the handling of TCN fingerprints:

- When the ECRIS TCN system triggers the dissemination of TCN information it needs to connect to the national AFIS for retrieving the TCN fingerprints. It pseudonymises and encrypts the fingerprints before sending them to all other Member States via the sTESTA network.
- When receiving pseudonymised, encrypted NIST files, the ECRIS TCN system of a Member State having opted for Scenario 1B first decrypts the NIST file and then connects to the national AFIS so

as to store them. Here also a unique technical reference is transmitted by the disseminating Member State along with the pseudonymised NIST file for later reuse.

Figure 13 illustrates the described process for Scenario 1B.

Figure 13 Process for dissemination of TCN identity information in Scenario 1B

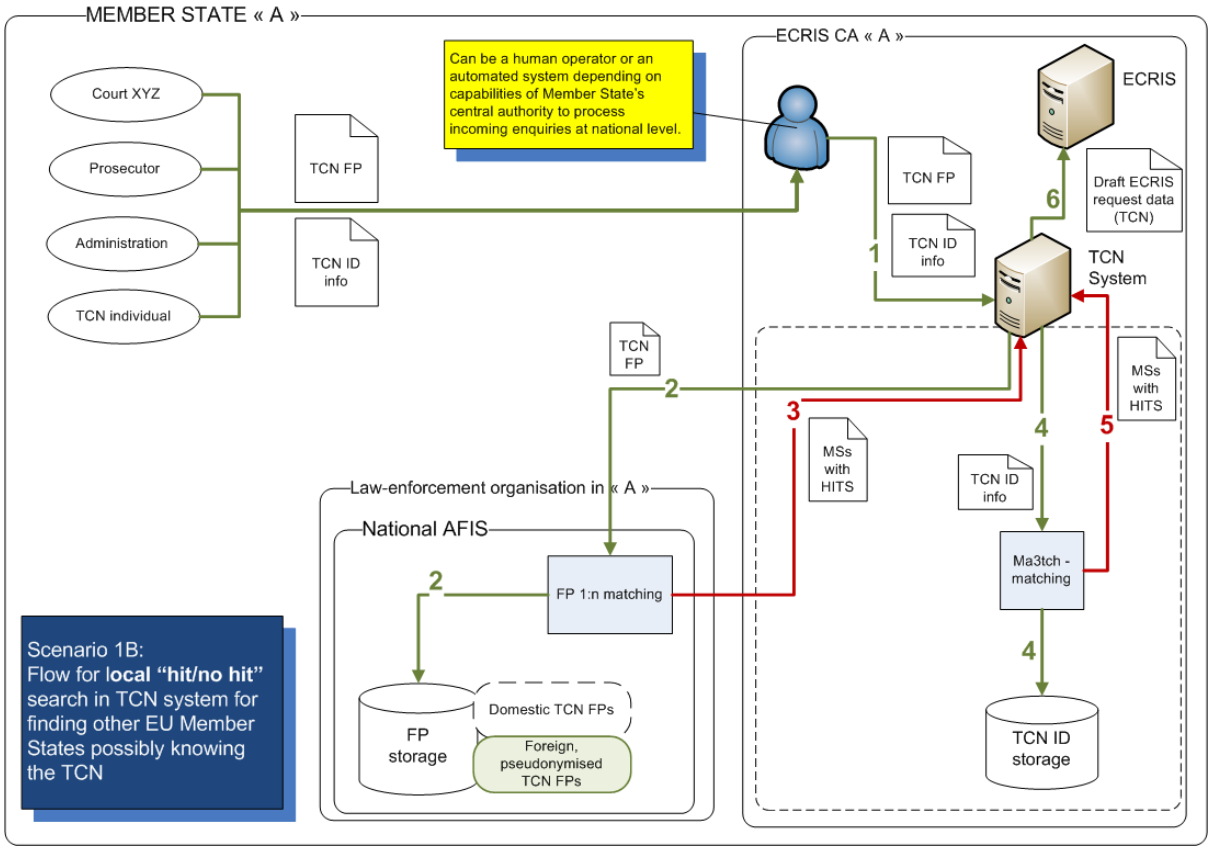


6.1.2.4 Process: local "hit/no hit" search for identifying Member States holding conviction data

The local "hit/no hit" search also works in a similar fashion as for Scenario 1A, with the exception that the ECRIS TCN system delegates the *one-to-many matching* using fingerprints to the national AFIS. Here also it must be assumed that the file given as input to the national AFIS is compliant with the ANSI NIST standard and that it contains high-quality fingerprint images.

The search based on alphanumeric identity information is performed by the ECRIS TCN system in the same way as in Scenario 1A, relying also on *ma3tch* algorithms. Figure 14 illustrates the described process for Scenario 1B.

Figure 14 Process for local "hit/no hit" search in Scenario 1B

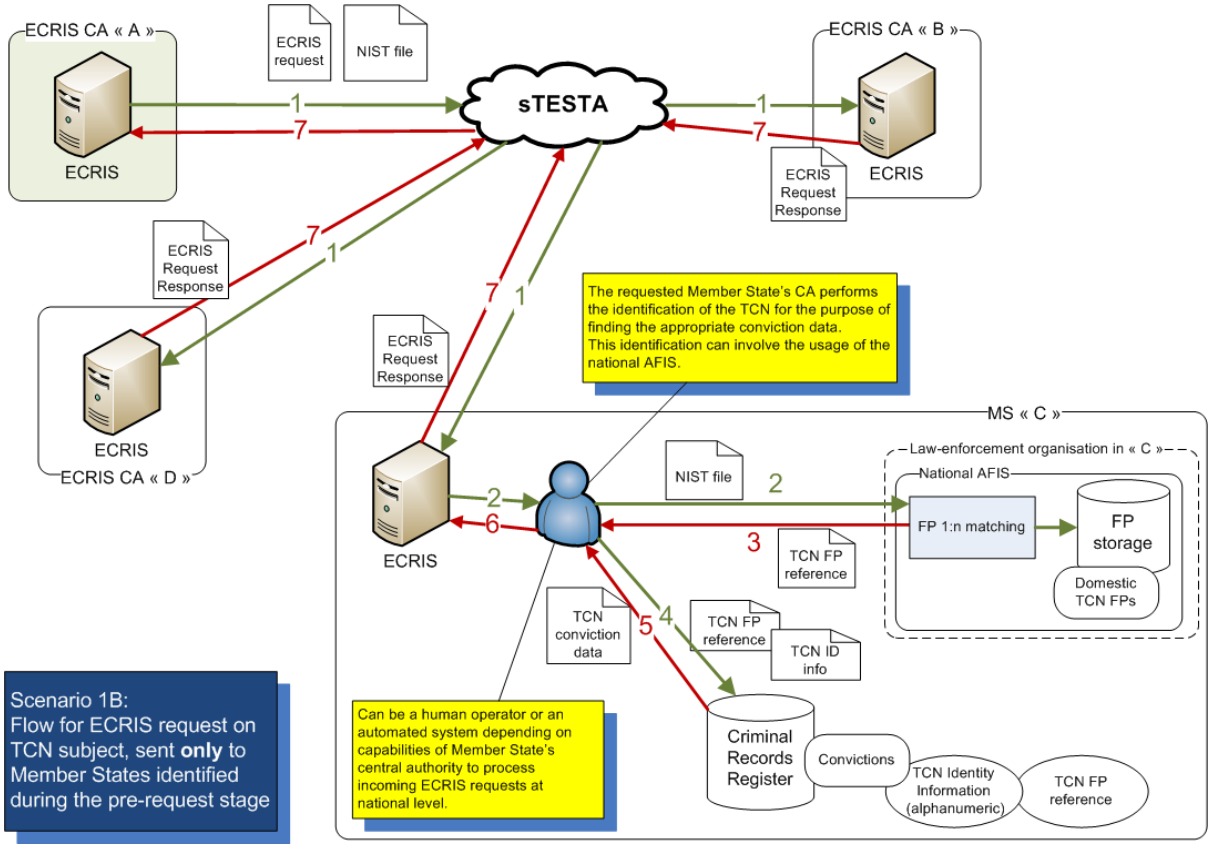


6.1.2.5 Process: ECRIS requests

As in Scenario 1A, the requesting Member State "A" sends an ECRIS request to each of the Member States identified by the previous "hit/no hit" search. In this scenario, the requested Member State that has opted for Scenario 1B is able to, in addition, rely on the capabilities of the national AFIS for performing additional searches and identity verification before actually extracting the conviction data from the criminal records register.

This has an additional benefit that the requested Member State could also rely on fingerprints captured and stored several years before the ECRIS TCN mechanism becomes operational, providing thus the possibility to find back convictions handed down even years ago. Figure 15 illustrates the described process for Scenario 1B.

Figure 15 Process for ECRIS request in Scenario 1B



6.2 Description of Scenario 2: decentralised ECRIS TCN system, no sharing of fingerprints and distributed "hit/no hit" search

Scenario 2 is based on the implementation of a **decentralised ECRIS TCN system** with the following key characteristics:

- Alphanumeric identity information of TCN convicted at national level is pseudonymised and systematically shared with all other Member States for storage in their national ECRIS TCN system.
- **Fingerprints of TCN** convicted at national level **are not shared** with all other Member States.
- A Member State searching for the past criminal history of a particular TCN performs a **distributed "hit/no hit" search** on fingerprints in the ECRIS TCN systems of all other member States for identifying which other Member State(s) can be queried for information about these past convictions.

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 ECRIS TCN system. The identity information and fingerprints are pseudonymised and stored locally, but the pseudonymised fingerprints are not transmitted to the other Member States.

When a Member State needs to search for information on past convictions for a given TCN, the CA of the requesting Member State uses its ECRIS TCN system to find whether this TCN is known within the EU. Specifically for searching using fingerprints, the ECRIS TCN system of the requesting Member State automatically contacts the ECRIS TCN systems of the 27 other Member States in order to perform a matching process and to find which other Member States have information on past convictions. The CA then prepares an ECRIS request and sends it to the list of Member States found previously by the ECRIS TCN system.

Several parts are identical with Scenarios 1A and 1B, and are thus not repeated in full detail:

- The overview of the modules.
- The process for storing information on a newly convicted TCN.
- The process for sending ECRIS requests to the Member States found during the “hit/no hit” search.

The main differences reside in the processes describing the dissemination of TCN identity information and in the “hit/no hit” search for finding the Member States to which the ECRIS request needs to be addressed.

6.2.1 Description of Scenario 2A

The following sections provide an overview of Scenario 2A and detail the main business processes regarding the exchange of information.

6.2.1.1 Overview

In Scenario 2A, the Member State does not rely on an existing national AFIS. Instead the ECRIS TCN system at national level needs to include a dedicated AFIS for the purpose of handling the TCN fingerprints.

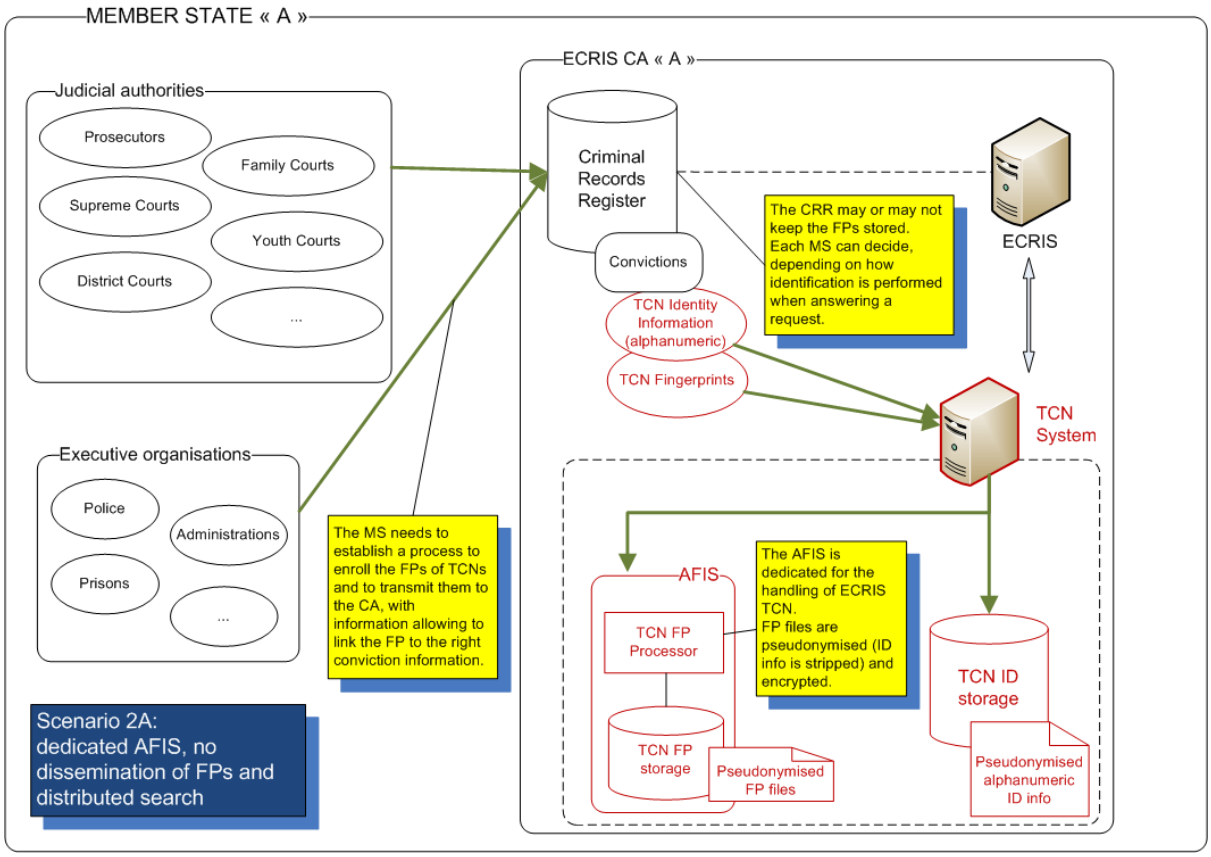
In this scenario the ECRIS TCN system is composed of:

- A dedicated AFIS which is composed of a server capable of processing fingerprint files and of the storage of the fingerprints.
- A TCN ID storage for processing, storing and matching alphanumeric identity information.

Please note here that the 2 components are completely separated and isolated in such a way that it is not possible to link the fingerprints kept in the AFIS to any identity information kept in the TCN ID storage. Both fingerprints and alphanumeric identity information are pseudonymised for protecting as much as possible the personal data.

The ECRIS TCN system looks similar to the one described for Scenario 1A. However the main difference is that fingerprints are not shared between Member States in this scenario. This implies that the dedicated AFIS contains only fingerprints of TCN convicted at national level and that the ECRIS TCN system, rather than disseminating fingerprints to all other Member States, needs to include functionality for supporting the distributed “hit/no hit” search as explained in the next sections. Figure 16 illustrates the overview of Scenario 2A.

Figure 16 Overview of Scenario 2A

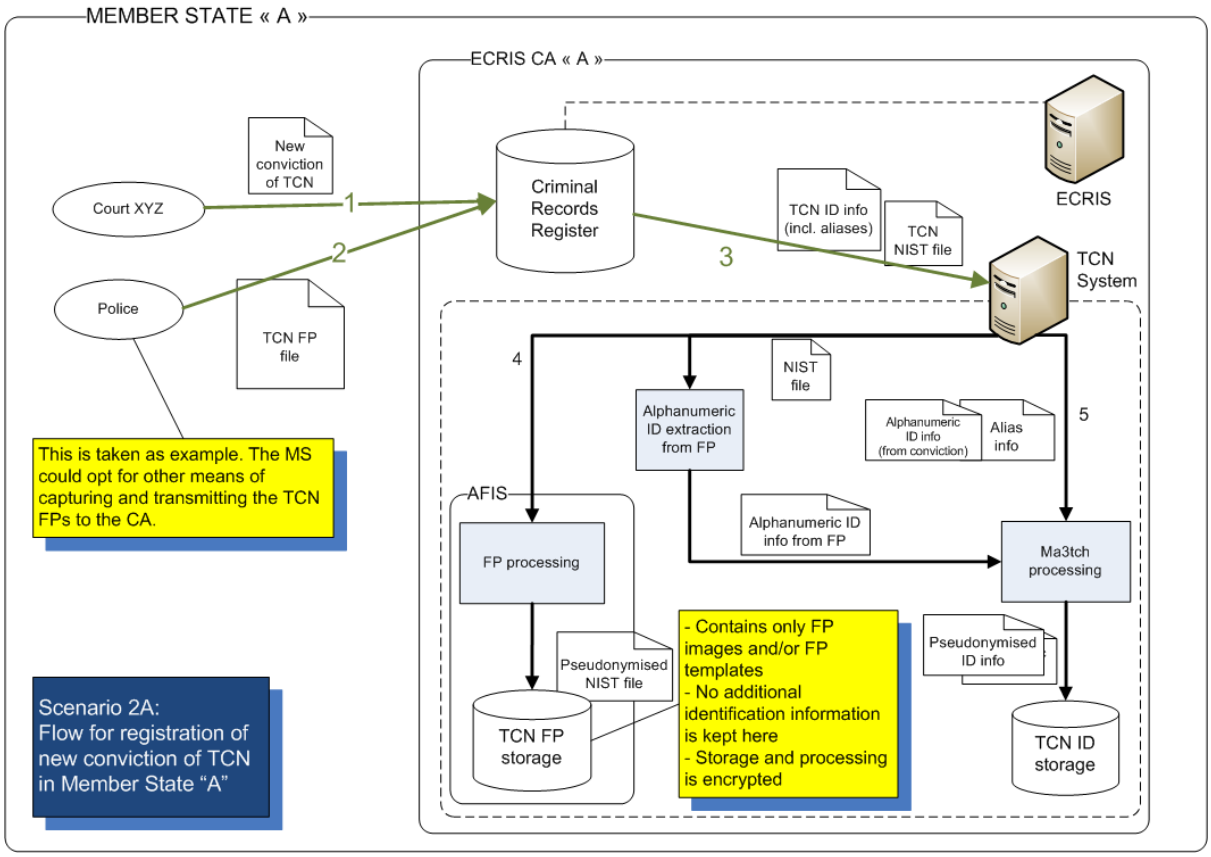


6.2.1.2 Process: new conviction of a TCN

This process works in exactly the same way as for Scenario 1A.

Here also the fingerprints provided by an executive organisation are entered by the CA into the ECRIS TCN system which pseudonymises and stores them into the internal AFIS. The alphanumeric identity information provided together with the conviction information is also entered by the CA into the ECRIS TCN system which runs it through a *ma3tch* pseudonymisation algorithm and stores it in the TCN ID storage. Figure 17 illustrates the described process for Scenario 2A.

Figure 17 Process for new conviction of a TCN in Scenario 2A

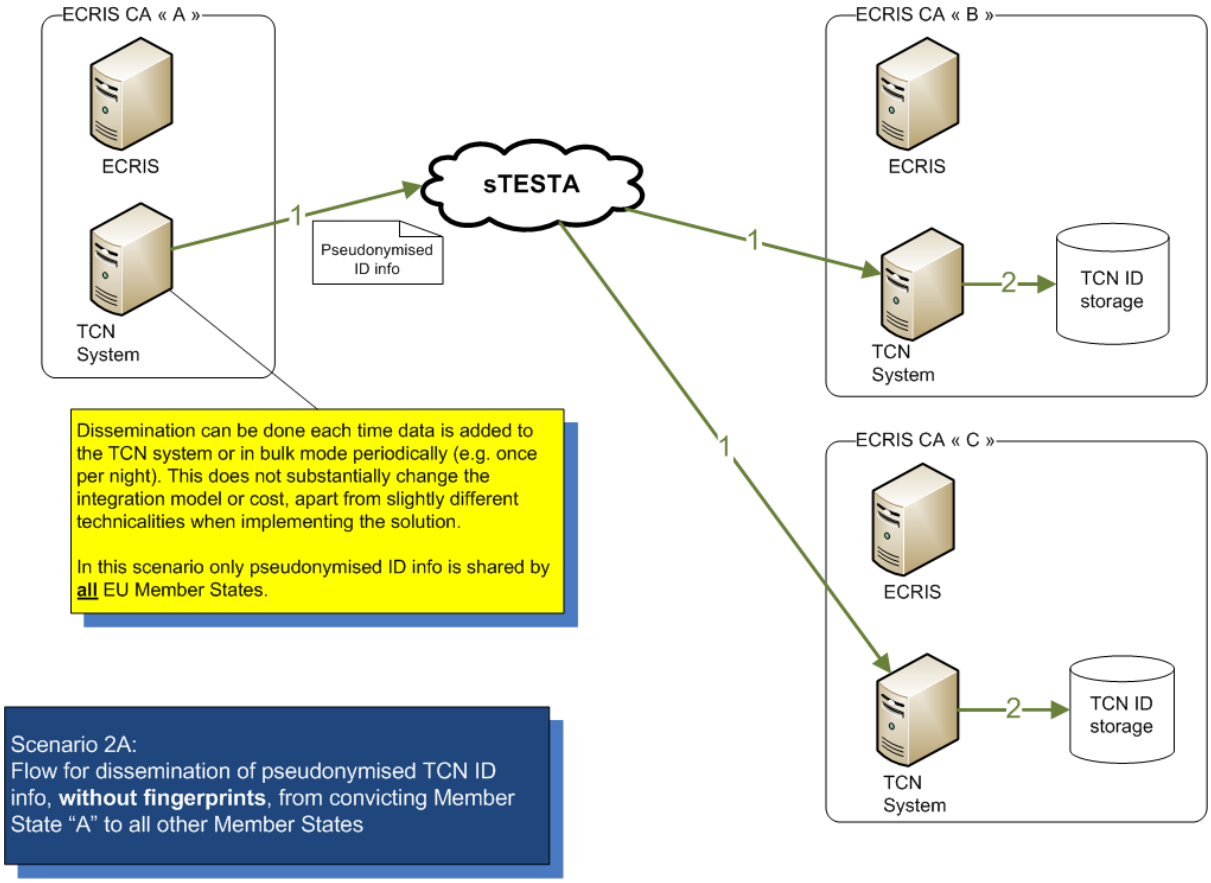


6.2.1.3 Process: dissemination of TCN identity information

The dissemination of TCN identity information differs from Scenario 1. Indeed in this scenario only the pseudonymised alphanumeric identity information is still shared with all other Member States. This relies on the existing *ma3tch* features for pseudonymisation and sharing of data through the secured sTESTA network.

Each Member State receiving the pseudonymised alphanumeric identity information stores it in its local TCN ID storage. Figure 18 illustrates the described process for Scenario 2B.

Figure 18 Process for dissemination of TCN identity information in Scenario 2A



6.2.1.4 Process: distributed "hit/no hit" search for identifying Member States holding conviction data

In this scenario the "hit/no hit" search for identifying Member States holding conviction information on a given TCN subject also differs from Scenarios 1A and 1B. As fingerprints are not shared between Member States, the ECRIS TCN system can only perform the look-up locally for the alphanumeric identity information but needs to interrogate the other 27 Member States for finding matches using fingerprints.

This process starts when a competent authority within the Member State contacts the CA to request information on past convictions for a given TCN. The authority provides the identity of the TCN as well as the fingerprints to the CA.

(1) In Member State "A", the CA enters the TCN identity information and fingerprints into the ECRIS TCN system in order to perform a "hit/no hit" search.

(2) The ECRIS TCN system injects the fingerprint file into the embedded AFIS. The AFIS first pseudonymises the fingerprint file by removing all alphanumeric identity information and encrypts it. (Here also, the fingerprint file is to be considered compliant with the ANSI NIST standard and containing tenprints images of high quality).

(3) Then the AFIS sends the encrypted NIST file to the ECRIS TCN systems of all other 27 Member States in order to trigger the *one-to-many matching* process. The file is sent through the secured sTESTA network, using the HTTPS protocol.

(4) In each of the 27 Member States, the ECRIS TCN system receives the pseudonymised NIST file and decrypts it. It passes it on to its embedded AFIS.

(5) Each queried AFIS performs the *one-to-many matching* and responds to the requesting ECRIS TCN system with a list of hits. For each "hit" the AFIS provides also the unique technical reference associated with the fingerprints that produced the "hit".

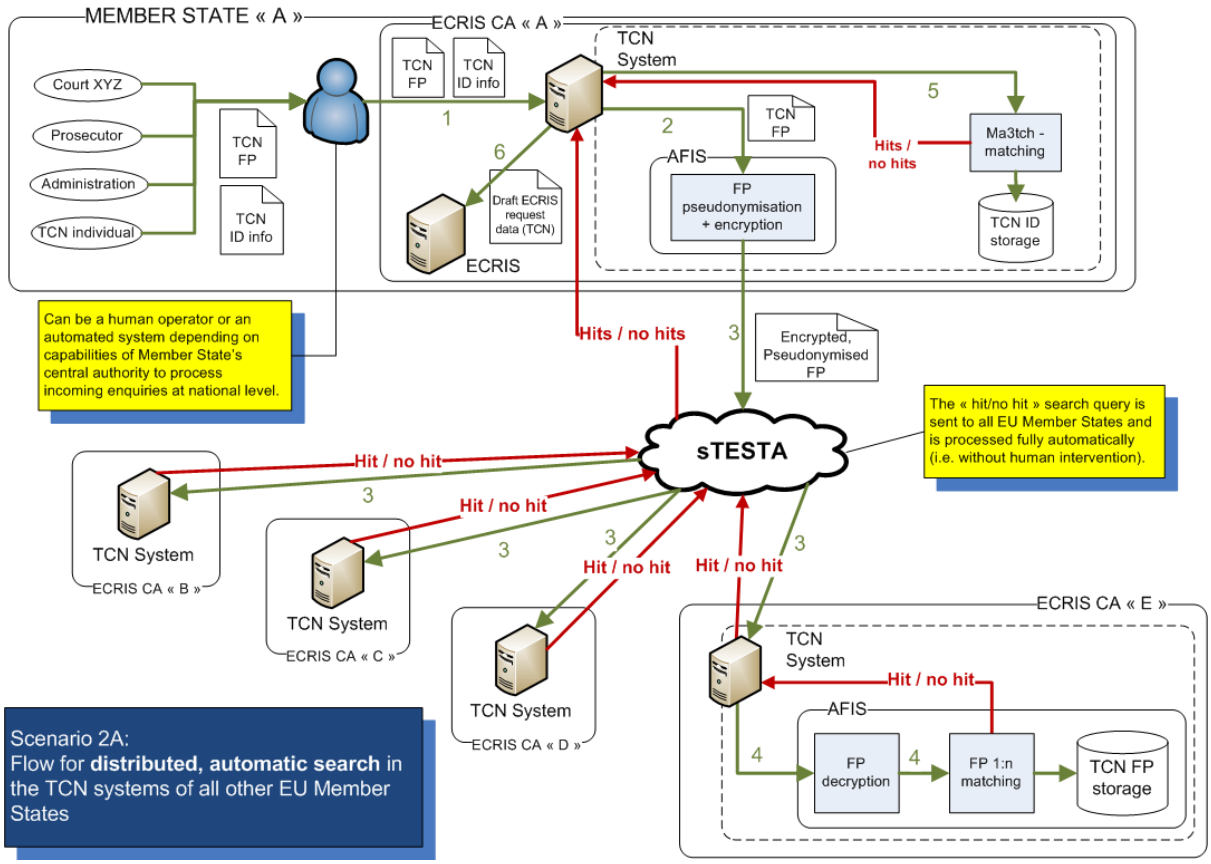
The ECRIS TCN system of the requesting Member State "A" collects and consolidates all "hit/no hit" replies from the 27 other Member States.

(6) The ECRIS TCN system of Member State "A" then also uses the alphanumeric ID info and performs a local matching using the *ma3tch* algorithms. The local TCN ID storage contains all entries of all EU countries; therefore this query does not need to be distributed. The *ma3tch* processor returns a list of Member States in which hits have been found.

(7) The ECRIS TCN system of Member State "A" finally consolidates the 2 lists of hits received from all other Member States and from the *ma3tch* processor. It prepares a draft ECRIS request message for each Member States having a "hit" and inputs these requests into ECRIS.

Figure 19 illustrates the described process for Scenario 2A.

Figure 19 Process for distributed "hit/no hit" search in Scenario 2A



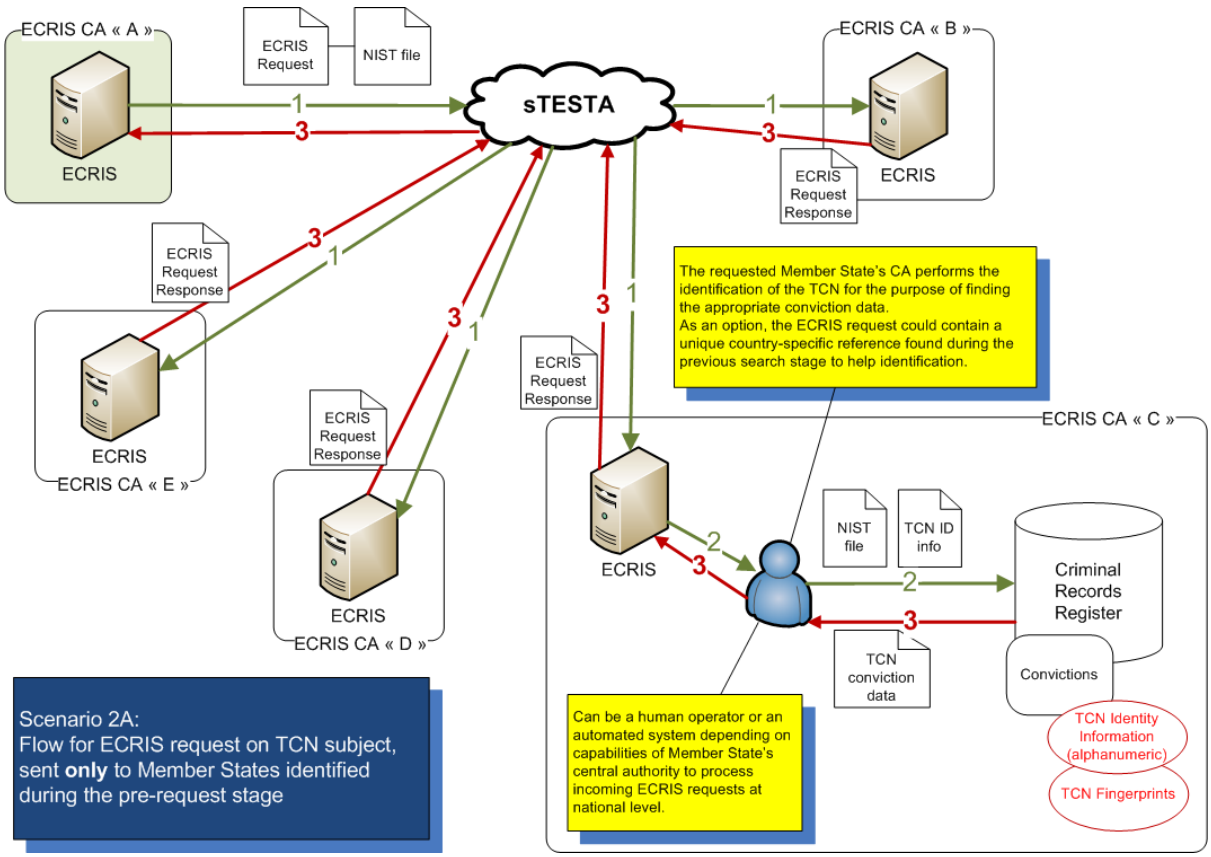
In this scenario it must be noted that the embedded AFIS of the requesting ECRIS TCN system needs to collect and consolidate 27 "hit/no hit" responses. The embedded AFIS thus also needs to perform error handling and needs to provide management of the 27 distinct calls so as to be able to gracefully handle situations such as loss of connectivity with other Member States, lack of "hit/no hit" within a given timeframe, etc.

6.2.1.5 Process: ECRIS requests

This process starts after the "hit/no hit" search has been done using the TCN identity information and fingerprints. At this moment the ECRIS TCN system has prepared draft ECRIS request messages.

The process of sending the ECRIS requests to the Member States identified previously and to respond to them is identical to Scenario 1A. Similarly as in Scenario 1A, the requested CA may use the AFIS that is included in the ECRIS TCN system for performing additional manual verifications using the fingerprints received together with the ECRIS request. The ECRIS request contains also the unique technical reference provided by the ECRIS TCN system when establishing the "hit", which can facilitate the extraction of the appropriate conviction information for the requested CA. Figure 20 illustrates the described process for Scenario 2A.

Figure 20 Process for ECRIS request in Scenario 2A



6.2.2 Description of Scenario 2B

In Scenario 2B, the Member State extends and reuses an existing national AFIS. The ECRIS TCN system at national level does not include a dedicated AFIS for the purpose of handling the TCN fingerprints but links with the national AFIS. It still contains the TCN ID storage and *ma3tch* processing features.

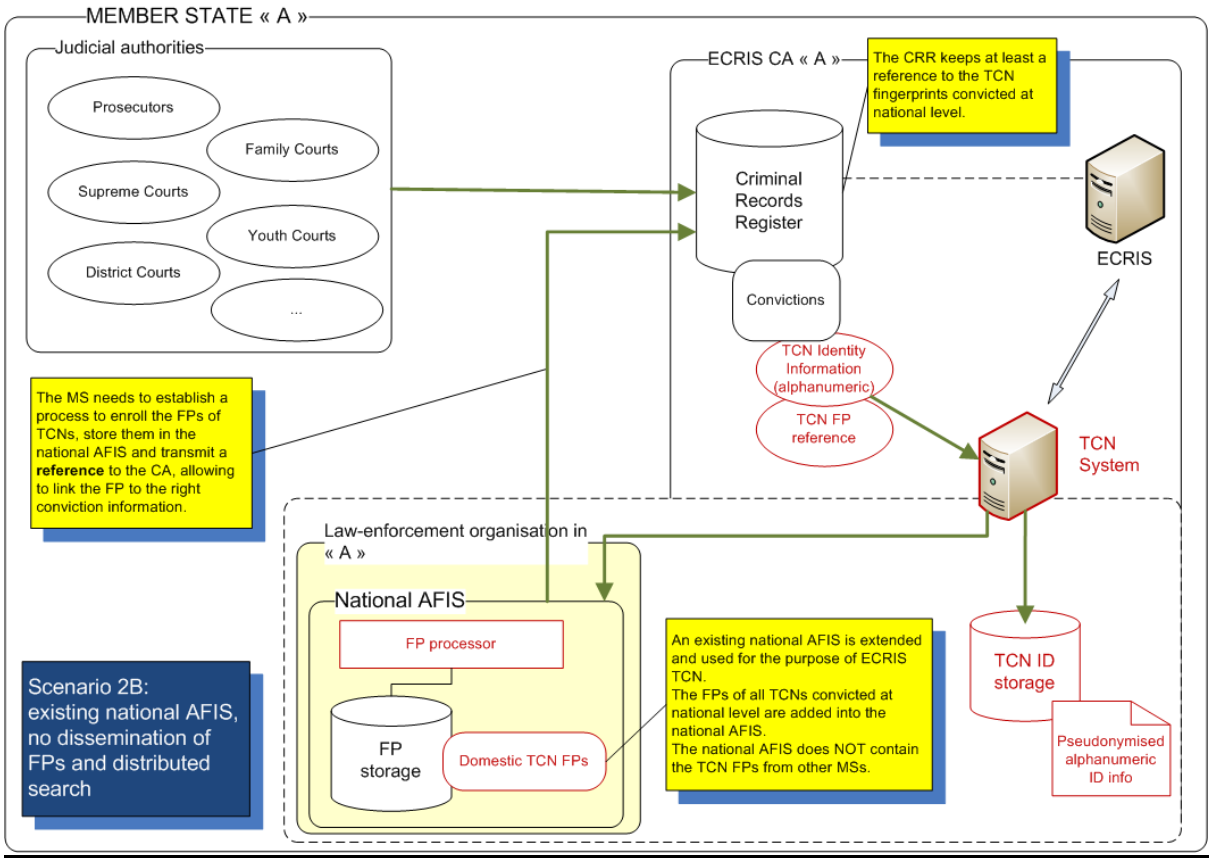
As stated previously, Member States may opt for Scenario 2A or 2B as both are interoperable and able to work together in the EU landscape.

6.2.2.1 Overview

The main difference with Scenario 2A is that the ECRIS TCN system does not contain its own dedicated AFIS but links with a national AFIS that is extended and reused for the purpose of handling the TCN fingerprints.

Similar to Scenario 1B, the national AFIS needs to be extended in such a way that it can include the fingerprints of TCN convicted at national level (labelled "domestic TCN fingerprints" in the diagram). However in this scenario the national AFIS does not receive and store the pseudonymised fingerprints of TCN convicted by all other EU Member States. Figure 21 illustrates the overview of Scenario 2B.

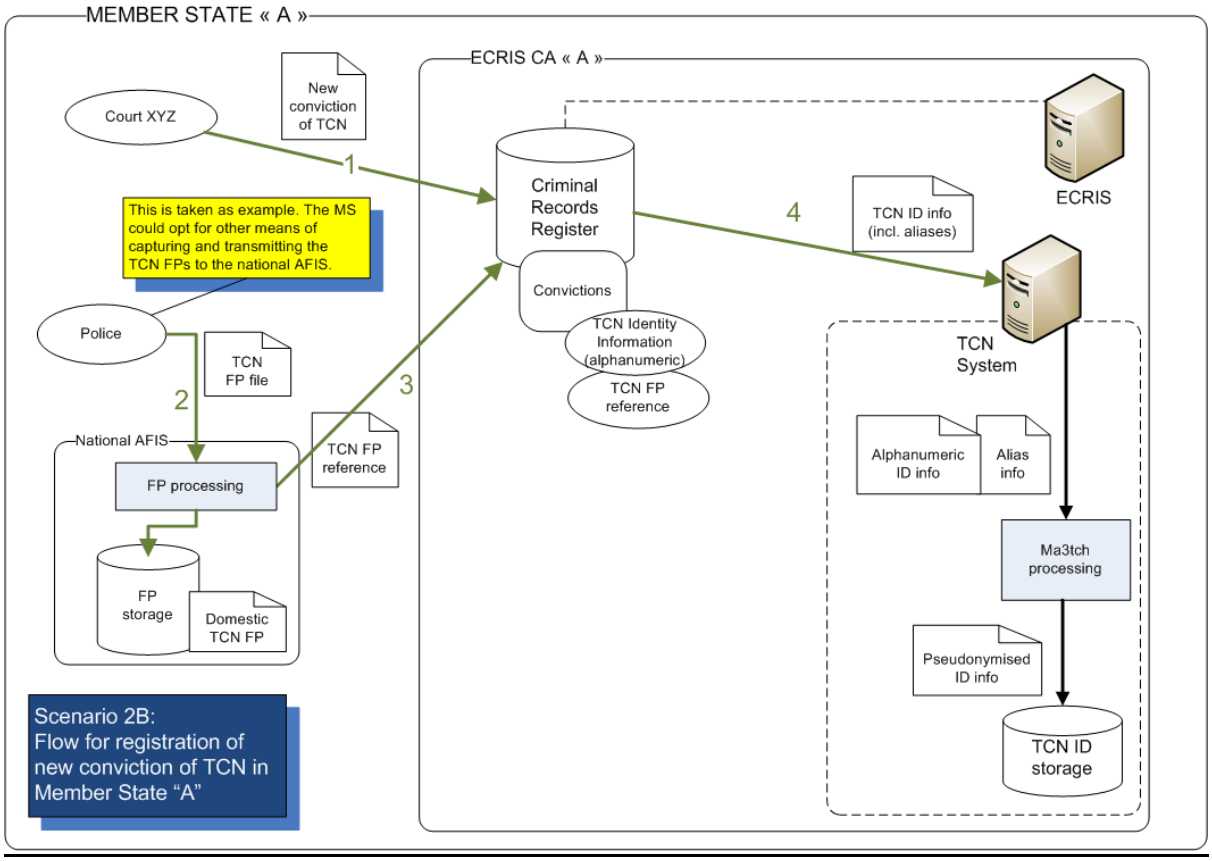
Figure 21 Overview of Scenario 2B



6.2.2.2 Process: new conviction of a TCN

This process is identical to the one presented in Scenario 1B. Here also the fingerprints taken from the convicted TCN are entered into the national AFIS, which then transmits at least a technical reference to the CA. The CA can then link this technical fingerprint reference to the TCN identity and conviction data in the criminal records register. As in Scenario 1B, the CA still feeds the alphanumeric identity information into the ECRIS TCN system which pseudonymises it using *ma3tch* algorithms and stores it in the TCN ID storage. Figure 22 illustrates the described process for Scenario 2B.

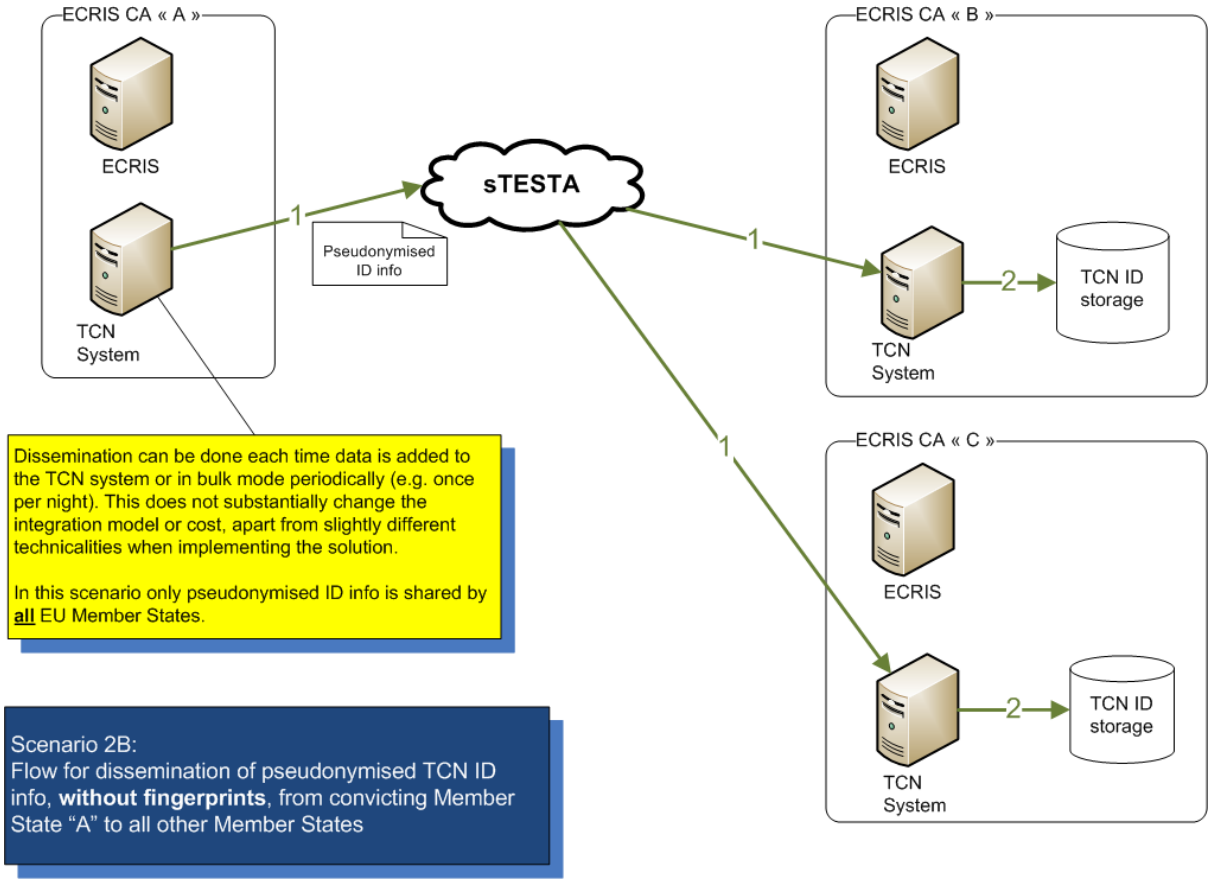
Figure 22 Process for new conviction of a TCN in Scenario 2B



6.2.2.3 Process: dissemination of TCN identity information

The dissemination of TCN identity information is identical to Scenario 2A. In this case only the alphanumeric identity information, pseudonymised using *ma3tch* algorithms, is distributed to all other Member States for storage in their ECRIS TCN system. Figure 23 illustrates the described process for Scenario 2B.

Figure 23 Process for dissemination of TCN identity information in Scenario 2B

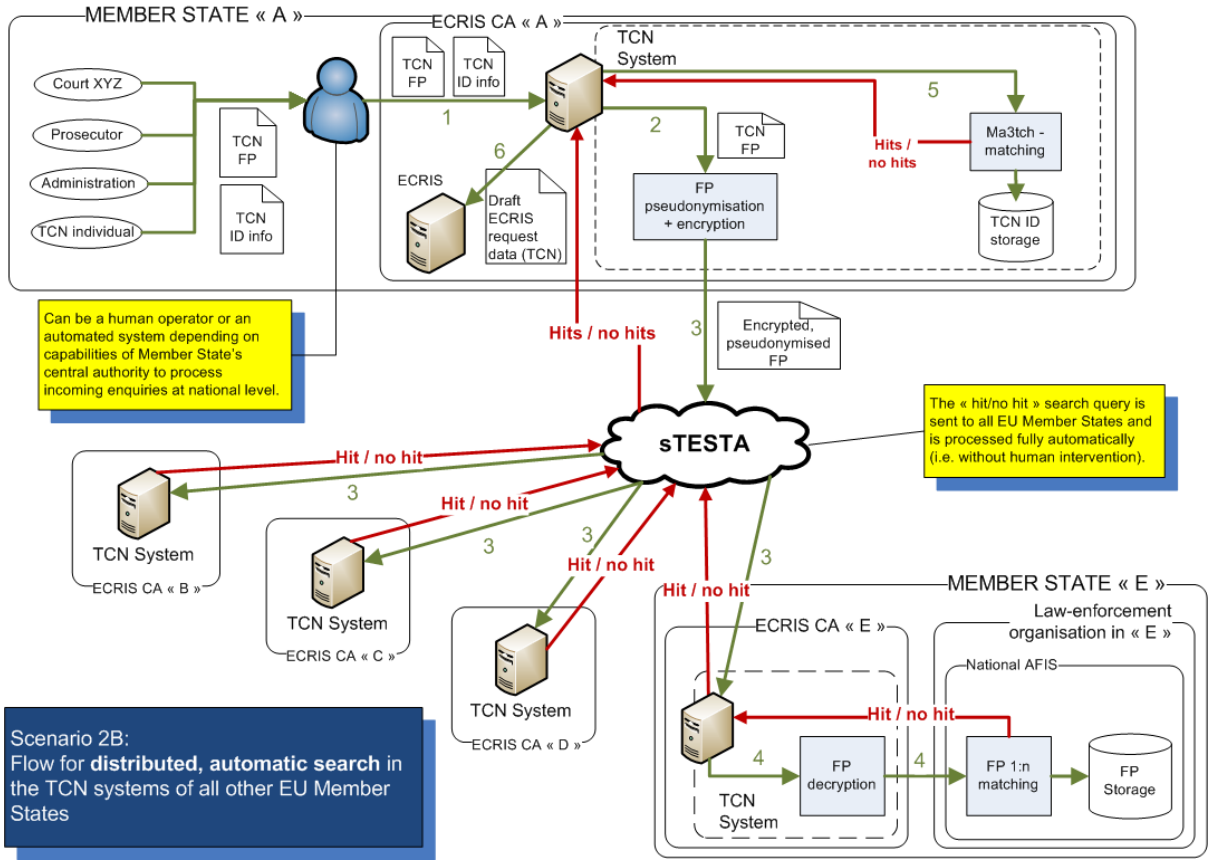


6.2.2.4 Process: distributed "hit/no hit" search for identifying Member States holding conviction data

The "hit/no hit" search mechanism is also identical with the one described in Scenario 2A.

As fingerprints are not shared, the ECRIS TCN system of the requesting CA automatically forwards the "hit/no hit" query to the ECRIS TCN systems of all 27 other Member States in order to determine which Member States hold past conviction information concerning the given TCN subject. As in Scenario 2A, the search based on alphanumeric identity information is done locally by the requesting CA using its own ECRIS TCN system. Figure 24 illustrates the described process for Scenario 2B.

Figure 24 Process for distributed "hit/no hit" search in Scenario 2B

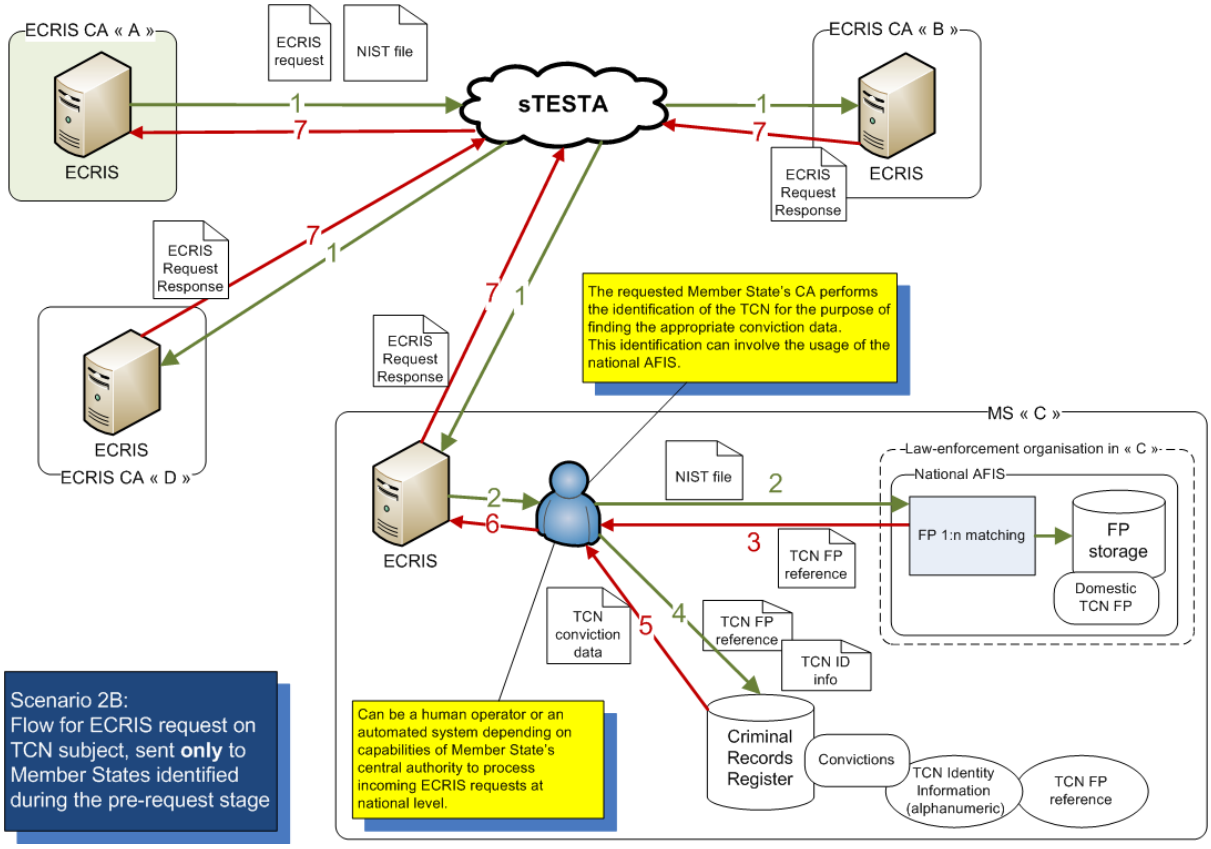


6.2.2.5 Process: ECRIS requests

As in the previous scenarios, the requesting Member State "A" sends an ECRIS request to each of the Member States identified by the previous "hit/no hit" search.

The requested Member State that has opted for Scenario 2B can in addition rely on the capabilities of the national AFIS for performing additional searches and identity verification before actually extracting the conviction data from the criminal records register. Figure 25 illustrates the described process for Scenario 2B.

Figure 25 Process for ECRIS request in Scenario 2B



6.3 Description of Scenario 3: central AFIS, sharing of alphanumeric data, "hit/no hit" search at central and local level

Scenario 3 is based on the implementation of a **centralised AFIS.** The scenario has the following key characteristics:

- Alphanumeric identity information of TCN convicted at national level is pseudonymised and systematically shared with all other Member States for storage in their national ECRIS TCN system.
- A **central AFIS** is put in place, under management of eu-LISA.
- **Pseudonymised fingerprints of TCN** convicted at national level **are stored in the central AFIS** 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 a **"hit/no hit" search on fingerprints in the central AFIS** for identifying which other Member State(s) can be queried for information on these past convictions.

In this scenario, the Member States do not share the fingerprints of the convicted TCN. They are rather centralised in an EU-wide AFIS 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 local ECRIS TCN system. The identity information is pseudonymised and shared with all other Member States whereas the fingerprints are pseudonymised and stored in the central AFIS.

When a Member State needs to collect information on past convictions for a given TCN, the CA of the requesting Member State uses its ECRIS TCN system to find whether this TCN is known within the EU. The ECRIS TCN system automatically contacts the central AFIS in order to perform a matching process to find which other Member States have information on past convictions. The search based on alphanumeric data is done locally by the ECRIS TCN system. The CA then prepares an ECRIS request based on the result of the “hit/no hit” search and sends it to the list of Member States found by the ECRIS TCN system.

6.3.1 Description of Scenario 3A

The following sections provide an overview of Scenario 3A and detail the main business processes regarding the exchange of information.

6.3.1.1 Overview

In this scenario the ECRIS TCN system at national level is composed of:

- The TCN FP storage: this part is not an AFIS but a technical component embedded within the TCN ECRIS system capable of pseudonymising and storing fingerprint files.
- The TCN ID storage for processing, storing and matching alphanumeric identity information

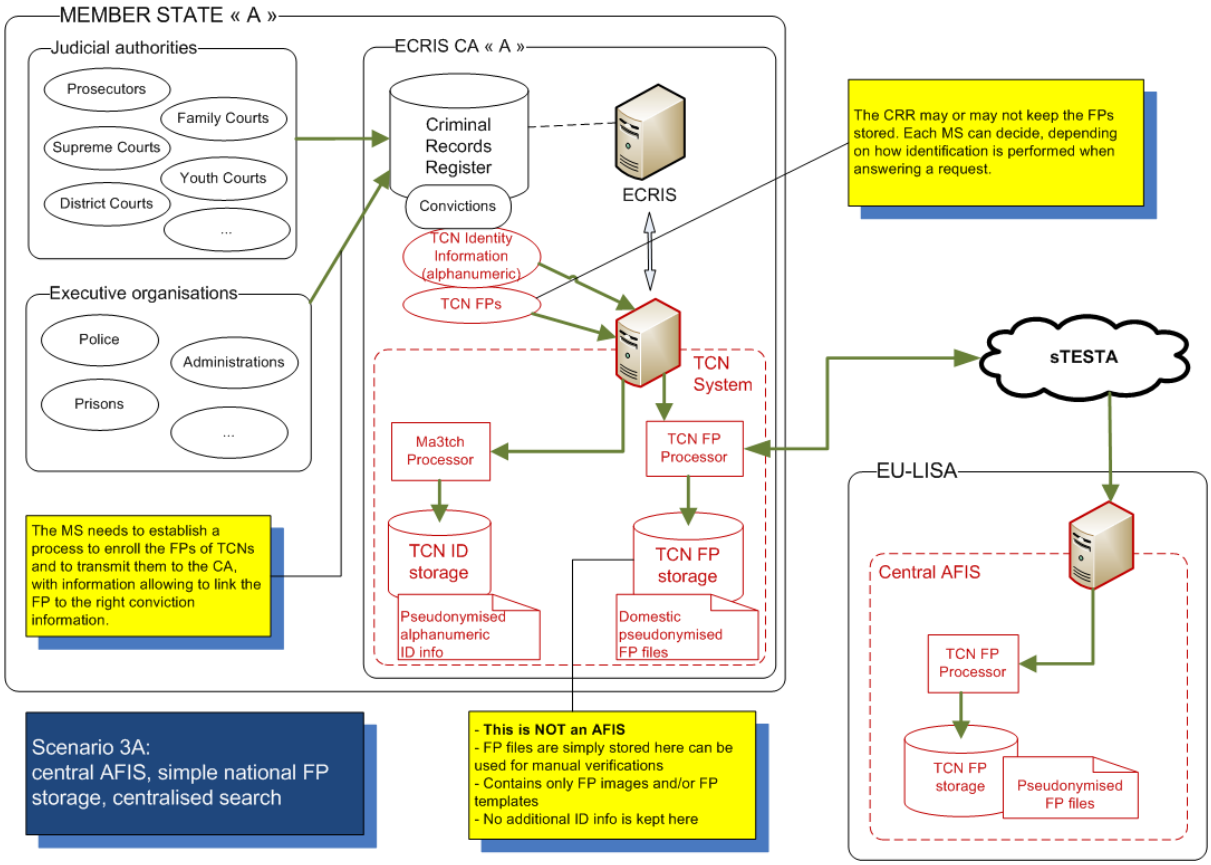
Please note here that the 2 components are completely separated and isolated in such a way that it is not possible to link the fingerprints kept in the TCN FP storage to any identity information kept in the TCN ID storage. Both fingerprints and alphanumeric identity information are pseudonymised for protecting as much as possible the personal data.

At EU-level a central AFIS, dedicated to the purpose of ECRIS TCN, is set-up and managed by eu-LISA.

The national ECRIS TCN system is interconnected with the ECRIS system at national level, with the central AFIS and with the ECRIS TCN systems of the other Member States.

In order to better understand the usage of the ECRIS TCN system, the following sections describe the relevant processes to be considered. Figure 26 illustrates the overview of Scenario 3A.

Figure 26 Overview of Scenario 3A



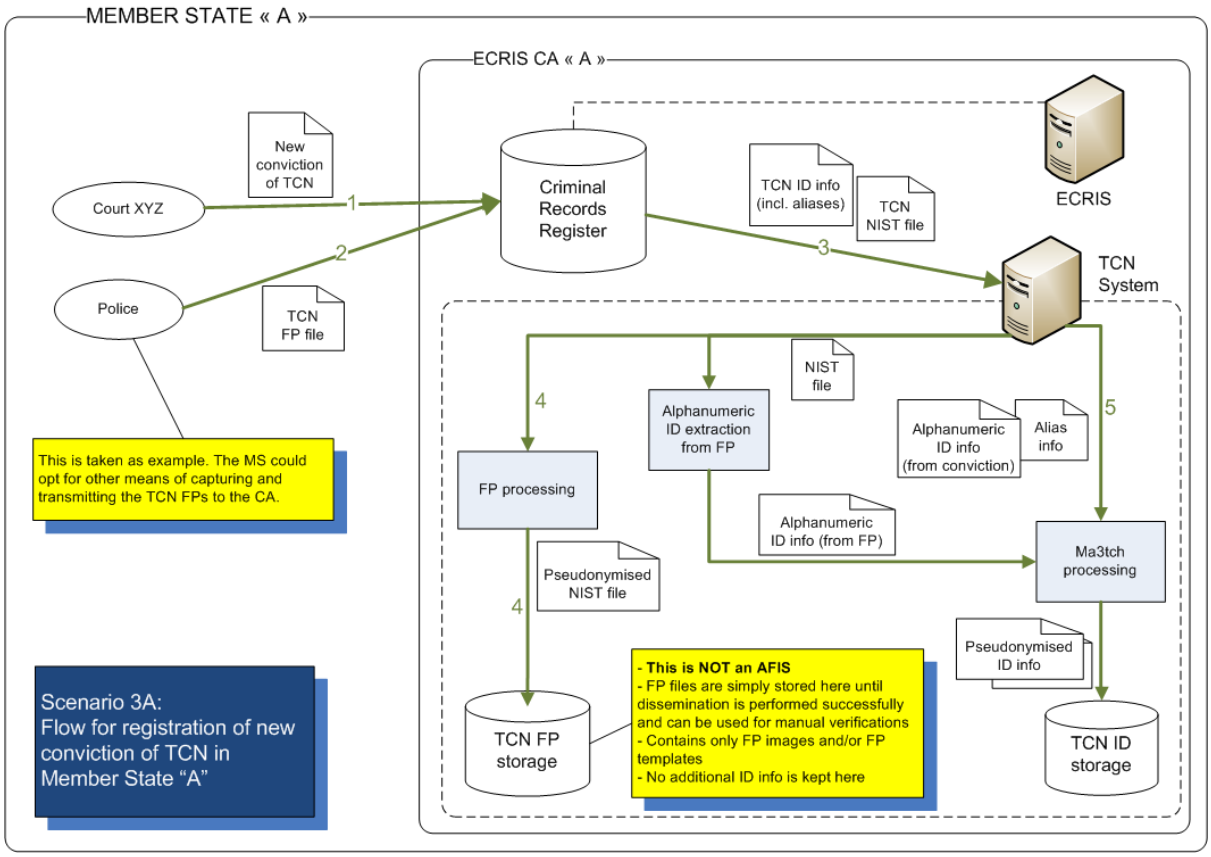
6.3.1.2 Process: new conviction of a TCN

This process works in a similar manner as for scenarios 1A and 2A.

The main difference here is that the ECRIS TCN system at national level does not embed a full AFIS but a simple storage system for the TCN fingerprints. When the CA feeds the TCN fingerprints into the ECRIS TCN system, it pseudonymises the fingerprint file, encrypts it and stores it.

Here again it is assumed that the fingerprints file collected at national level and provided as input to the CA are compliant with ANSI NIST standard and are of high quality. Figure 27 illustrates the described process for Scenario 3A.

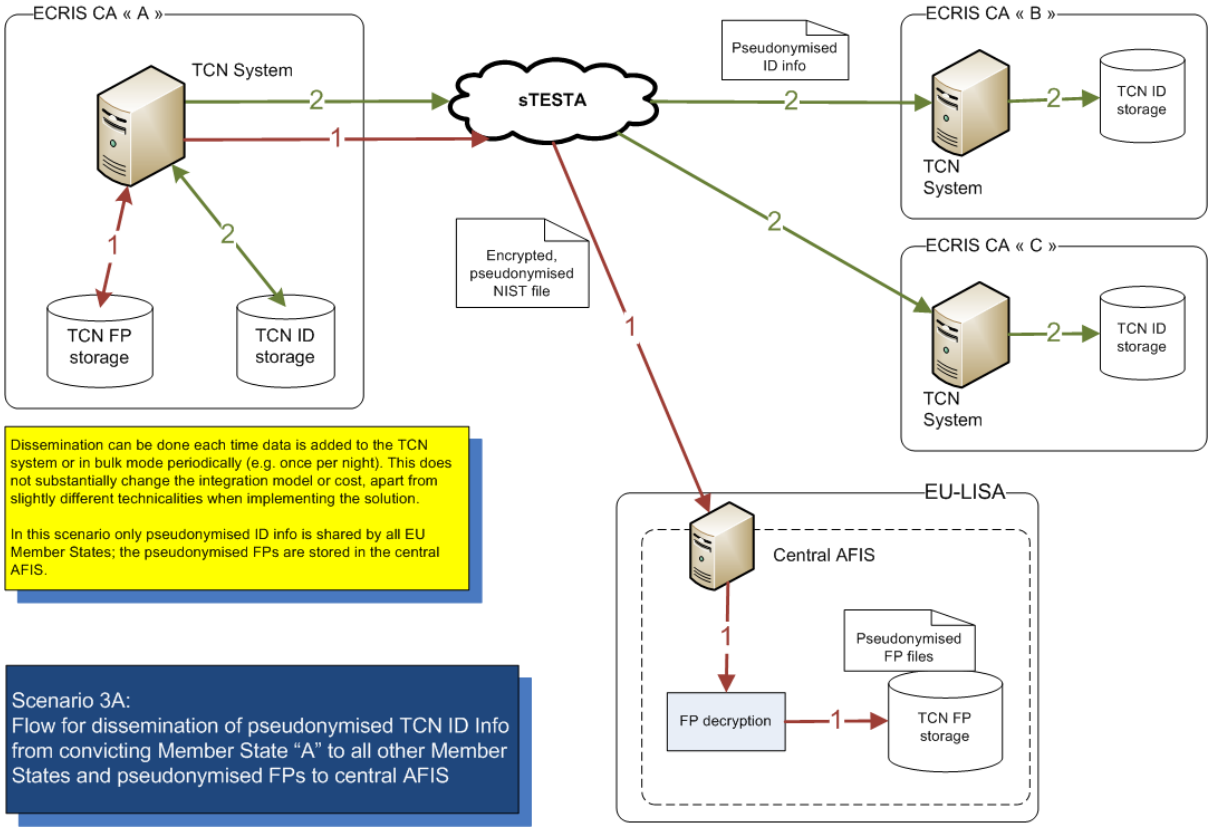
Figure 27 Process for new conviction of a TCN in Scenario 3A



6.3.1.3 Process: dissemination of TCN identity information

The dissemination of TCN identity information differs from the previous scenarios for fingerprints: the alphanumeric identity information is still pseudonymised using ma3tch algorithms and transmitted to all other Member States. The fingerprints however are encrypted and transmitted to the central AFIS through the sTESTA network. The central AFIS decrypts the fingerprints and stores them in such a way that they can be used for *one-to-many matching* with a maximum degree of accuracy. Figure 28 illustrates the described process for Scenario 3A.

Figure 28 Process for dissemination of TCN identity information in Scenario 3A



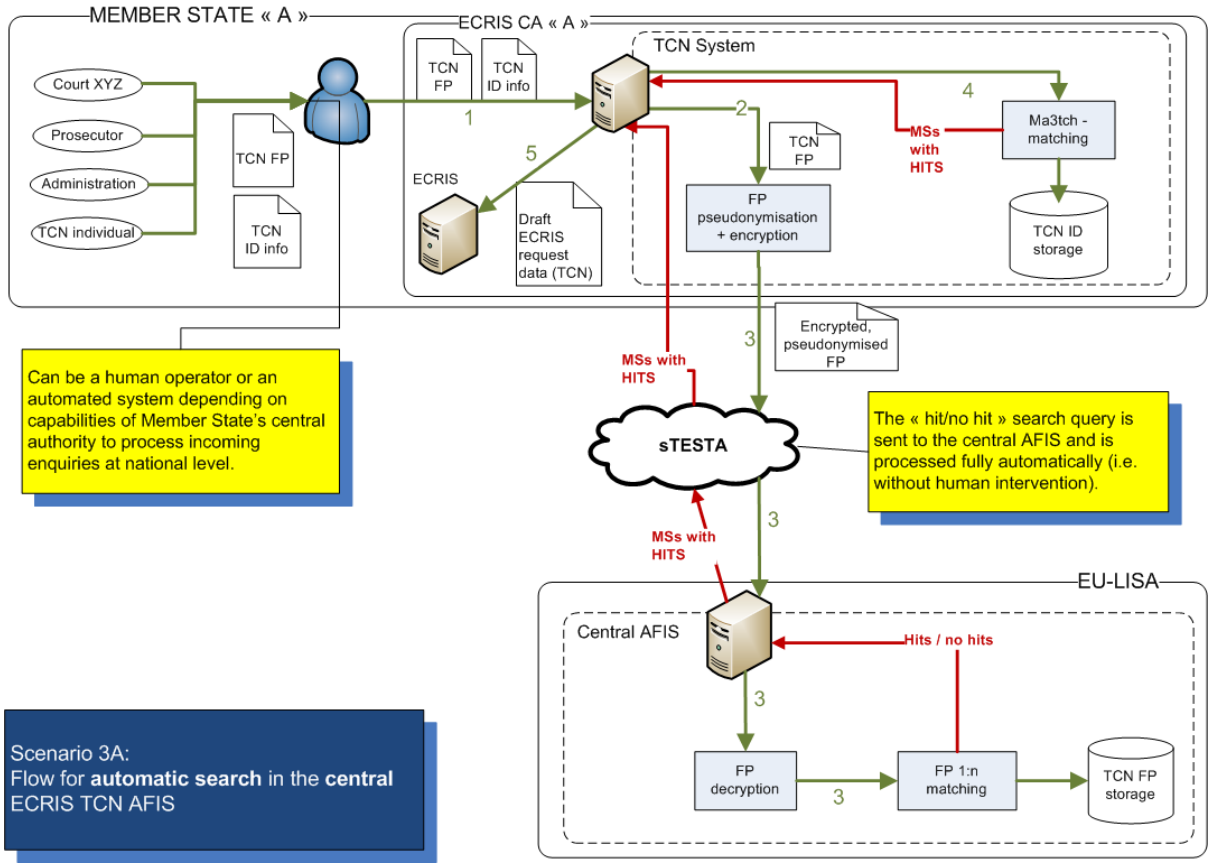
6.3.1.4 Process: central and local "hit/no hit" search for identifying Member States holding conviction data

In this scenario the "hit/no hit" search mechanism that aims at identifying the Member State(s) holding information on past convictions of a given TCN subject needs to rely on the central AFIS when using fingerprints. The search based on the alphanumeric identity information is still done locally within the ECRIS TCN system of the requesting CA.

When using the fingerprints of the TCN, the ECRIS TCN system of the requesting CA automatically pseudonymises and encrypts the fingerprints file and forwards it to the central AFIS via the secured sTESTA network. The central AFIS decrypts the received NIST file and performs a *one-to-many matching* against the fingerprints stored centrally. The central AFIS extracts the Member State and the unique technical reference for each fingerprint file that raised a "hit" and provides this as a response to the requesting ECRIS TCN system. As in previous scenarios, the search based on alphanumeric identity information is still handled locally by the ECRIS TCN system of the requesting CA as it contains the pseudonymised identity information collected from all Member States.

The requesting ECRIS TCN system then consolidates the lists of hits received from the central AFIS and from the local search on alphanumeric identity information and automatically generates draft ECRIS requests targeting the Member States that were identified. Figure 29 illustrates the described process for Scenario 3A.

Figure 29 Process for central and local "hit/no hit" search in Scenario 3A



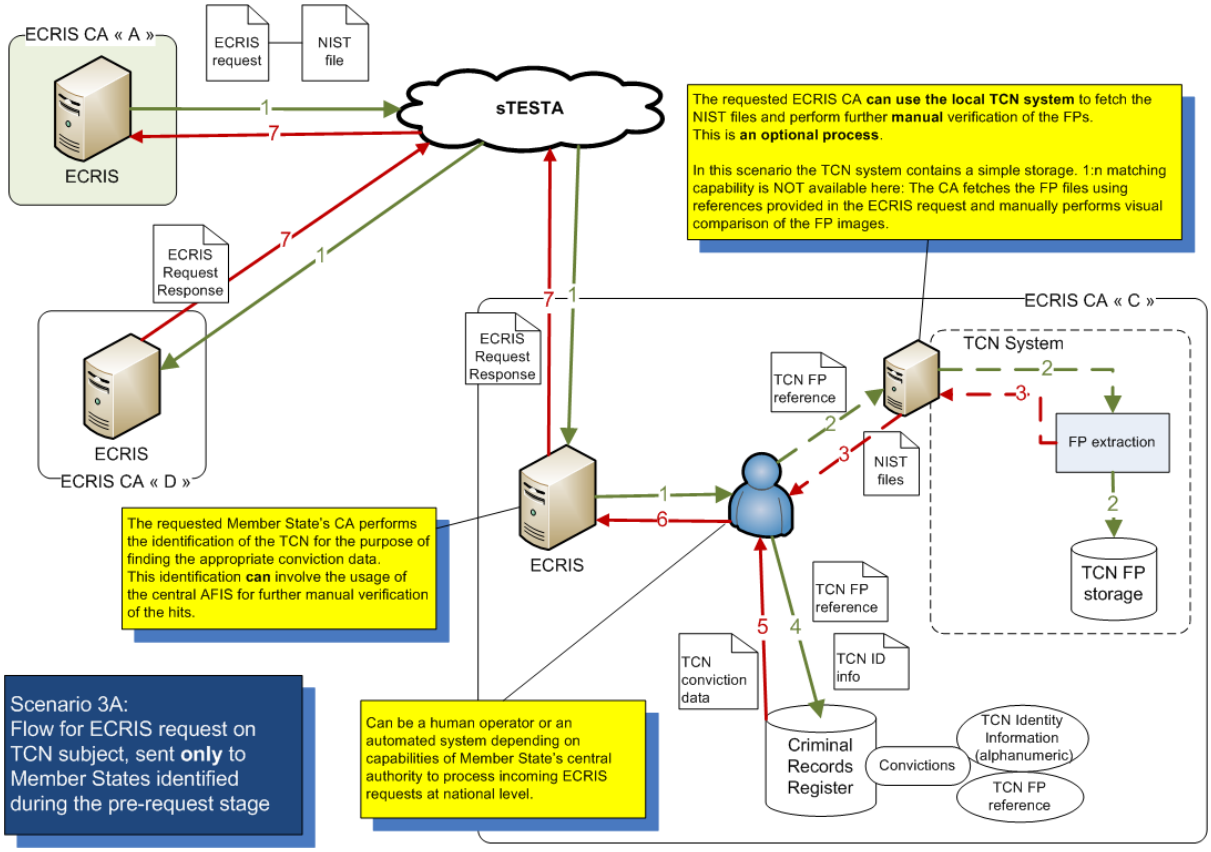
6.3.1.5 Process: ECRIS requests

The process of sending the ECRIS request to the Member States identified during the previous "hit/no hit" search and to respond to them is very similar to the previous scenarios.

The main difference is that in addition the requested CA is able to use the local ECRIS TCN system in order to extract the matching fingerprints for performing additional manual verifications for identifying the TCN subject. Please note however that the TCN FP storage contained in the ECRIS TCN system is not a full AFIS and thus does not provide advanced functionality for facilitating this verification. It is thus limited to the simple visualisation and comparison of fingerprint images without additional software features to assist in this task.

As in previous scenarios, the unique technical reference associated with the fingerprints that raised hits are also transmitted along with the ECRIS request and make it easier for the requested CA to find back the appropriate conviction data. Figure 30 illustrates the described process for Scenario 3A.

Figure 30 Process for ECRIS request in Scenario 3A



6.3.2 Description of Scenario 3B

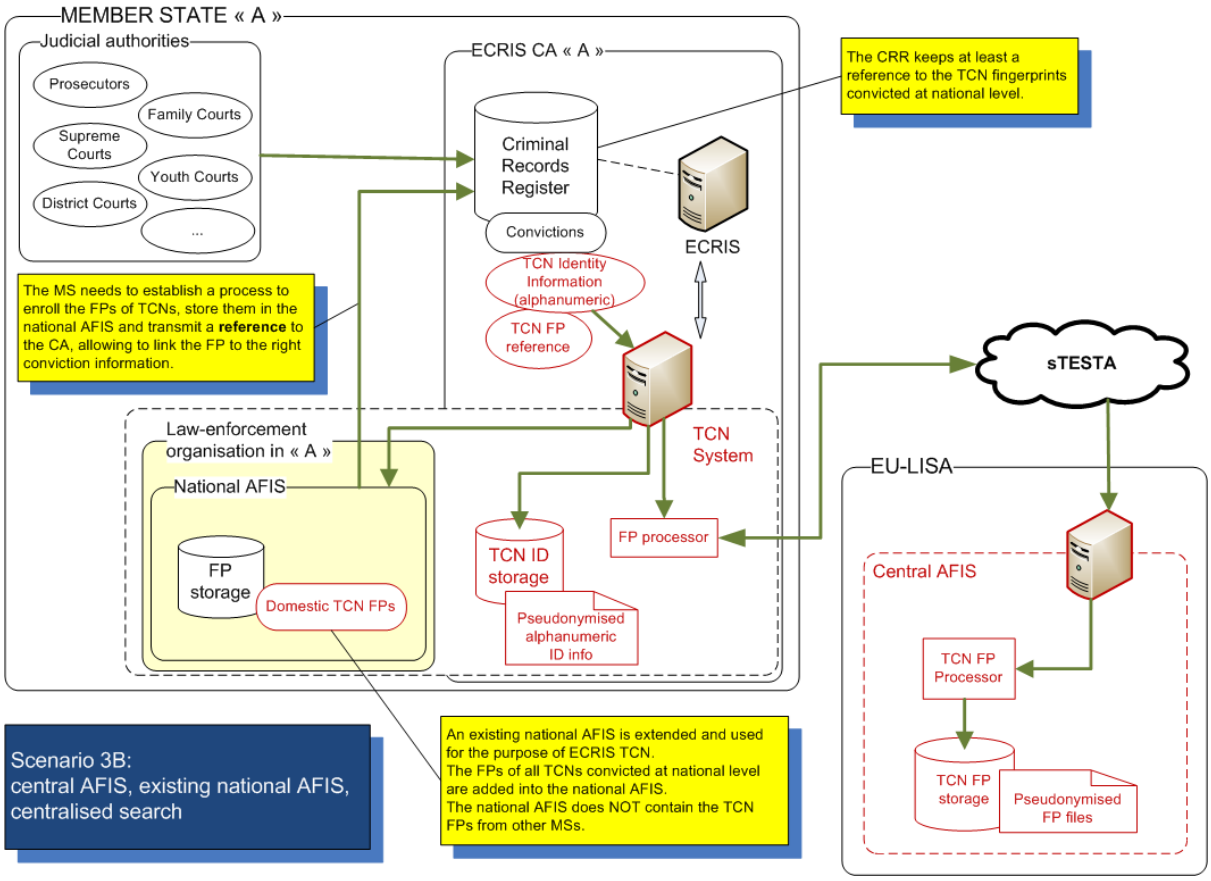
The following sections provide an overview of Scenario 3B and detail the main business processes regarding the exchange of information.

6.3.2.1 Overview

The main difference with Scenario 3A is that the ECRIS TCN system does not contain its own dedicated fingerprint storage but links with a national AFIS that is extended and reused for the purpose of handling the TCN fingerprints.

Similar to Scenario 2B, the national AFIS needs to be extended in such a way that it can include the fingerprints of TCN convicted at national level (labelled “domestic TCN fingerprints” in the diagram). Here also the national AFIS does not receive and store the pseudonymised fingerprints of TCN convicted by all other EU Member States, as they are all stored in the central AFIS managed by eu-LISA. The ECRIS TCN system still contains the necessary technical components for processing, disseminating and storing the alphanumerical identity information. Figure 33 illustrates the overview of Scenario 3B.

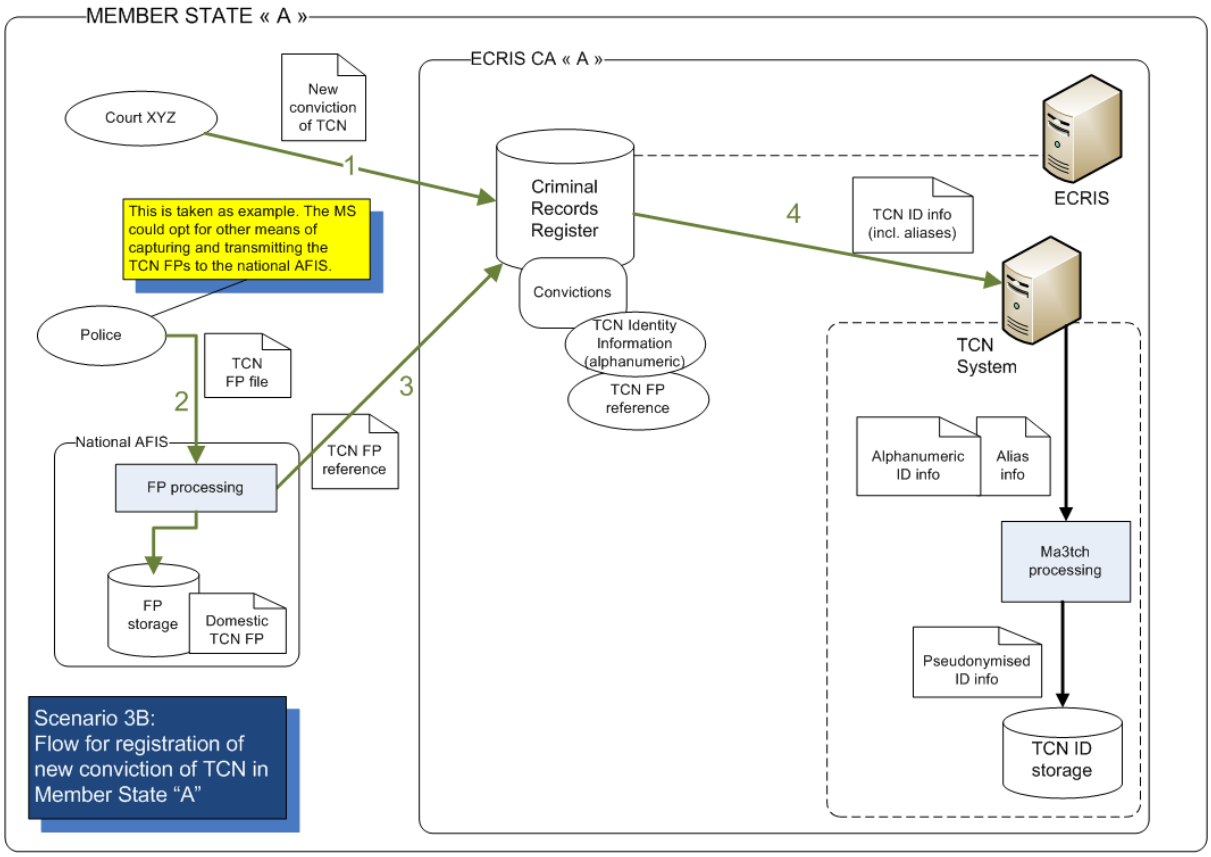
Figure 31 Overview of Scenario 3B



6.3.2.2 Process: new conviction of a TCN

This process is identical to the one presented in Scenario 2B. Here also the fingerprints taken from the convicted TCN are entered into the national AFIS, which then transmits at least a technical reference to the CA. The CA can then link this technical fingerprint reference to the TCN identity and conviction data in the criminal records register. As in Scenario 2B, the CA still feeds the alphanumeric identity information into the ECRIS TCN system which pseudonymises it using *ma3tch* algorithms and stores it in the TCN ID storage. Figure 32 illustrates the described process for Scenario 3B.

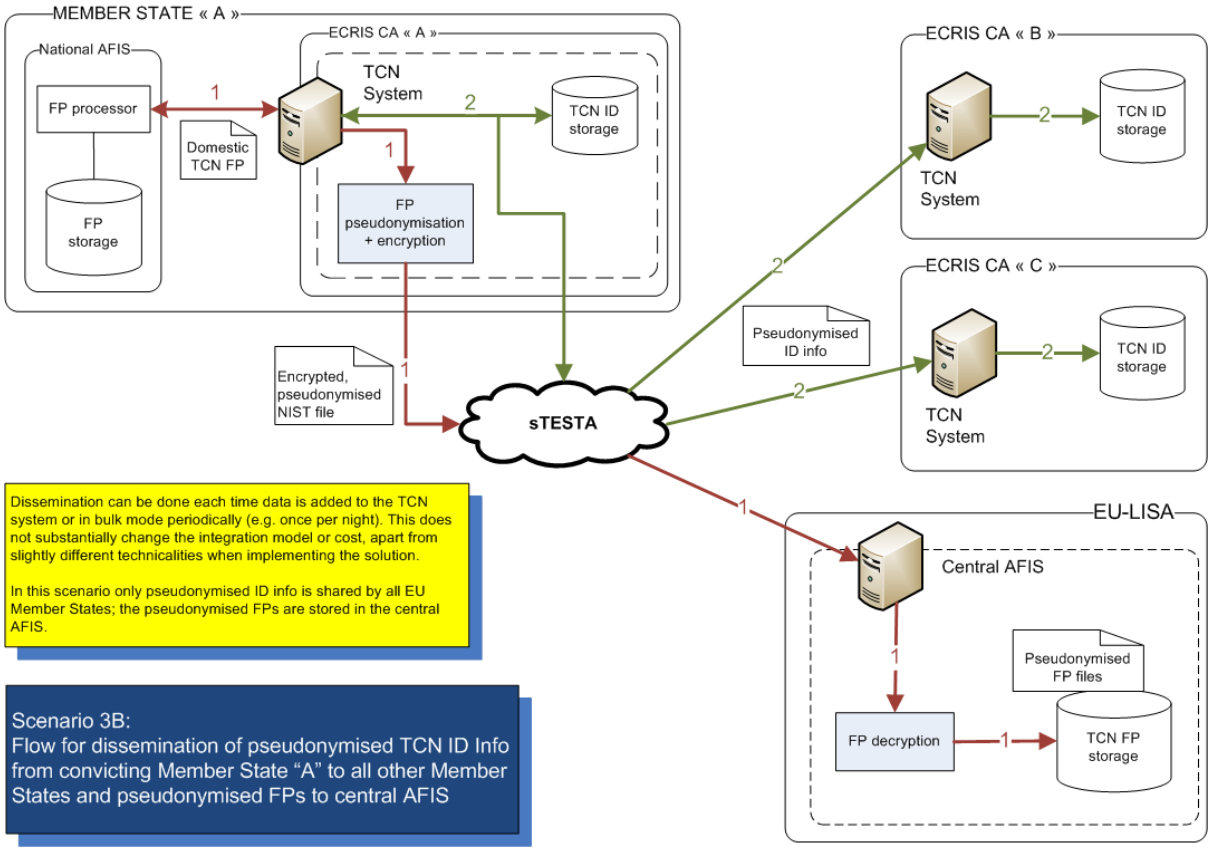
Figure 32 Process for new conviction of a TCN in Scenario 3B



6.3.2.3 Process: dissemination of TCN identity information

The dissemination of TCN identity information is identical as in Scenario 3A with the exception that the ECRIS TCN system needs to connect to the national AFIS in order to fetch the fingerprint files to be sent. As in Scenario 3A, the ECRIS TCN system then pseudonymises and encrypts the fingerprints and transmits the NIST file to the central AFIS for storage. As in the previous scenarios, the alphanumeric identity information is here also pseudonymised and shared with all other Member States. Figure 33 illustrates the described process for Scenario 3B.

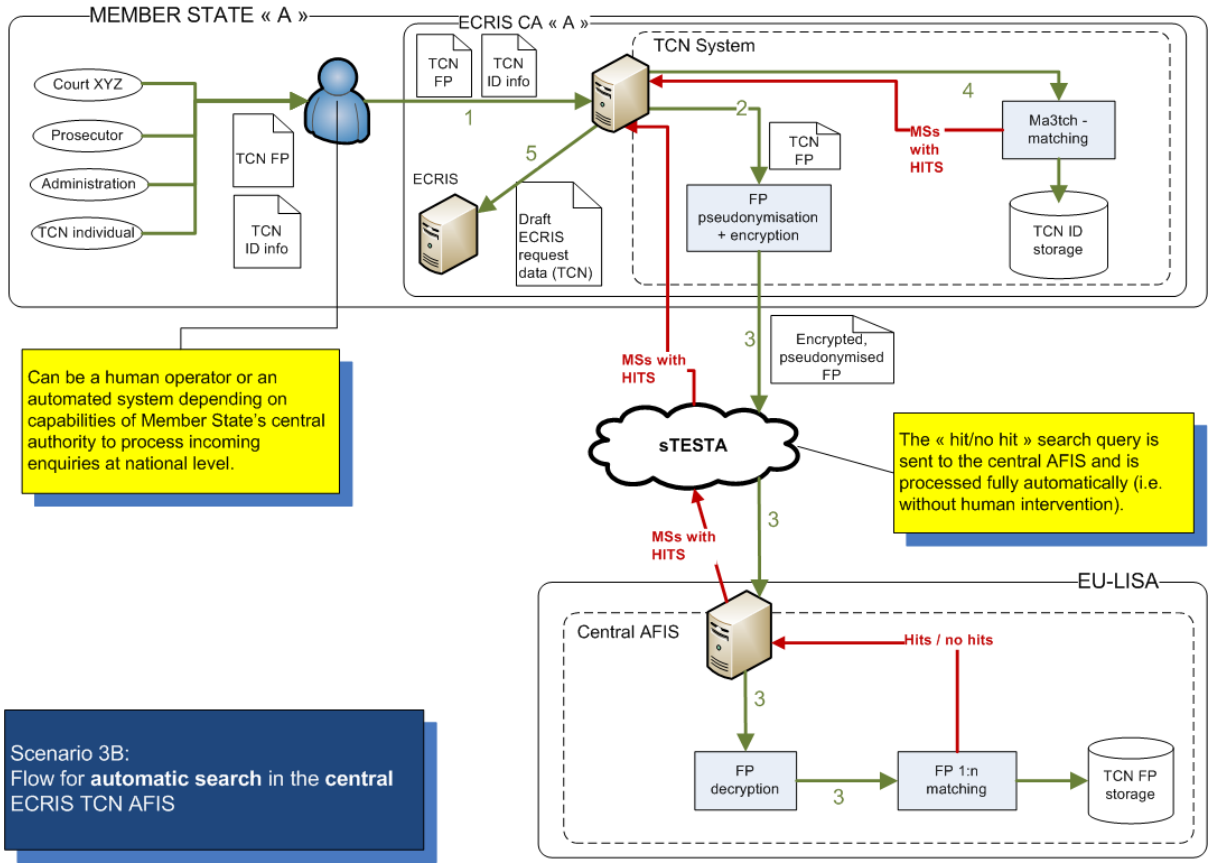
Figure 33 Process for dissemination of TCN identity information in Scenario 3B



6.3.2.4 Process: central and local "hit/no hit" search for identifying Member States holding conviction data

The "hit/no hit" search is identical to the one described in Scenario 3A. Here also the ECRIS TCN system automatically performs the search on alphanumeric identity information locally against the identities kept in the TCN ID storage, whereas it uses the central AFIS in order to trigger the *one-to-many matching* using the TCN fingerprints. Figure 34 illustrates the described process for Scenario 3B.

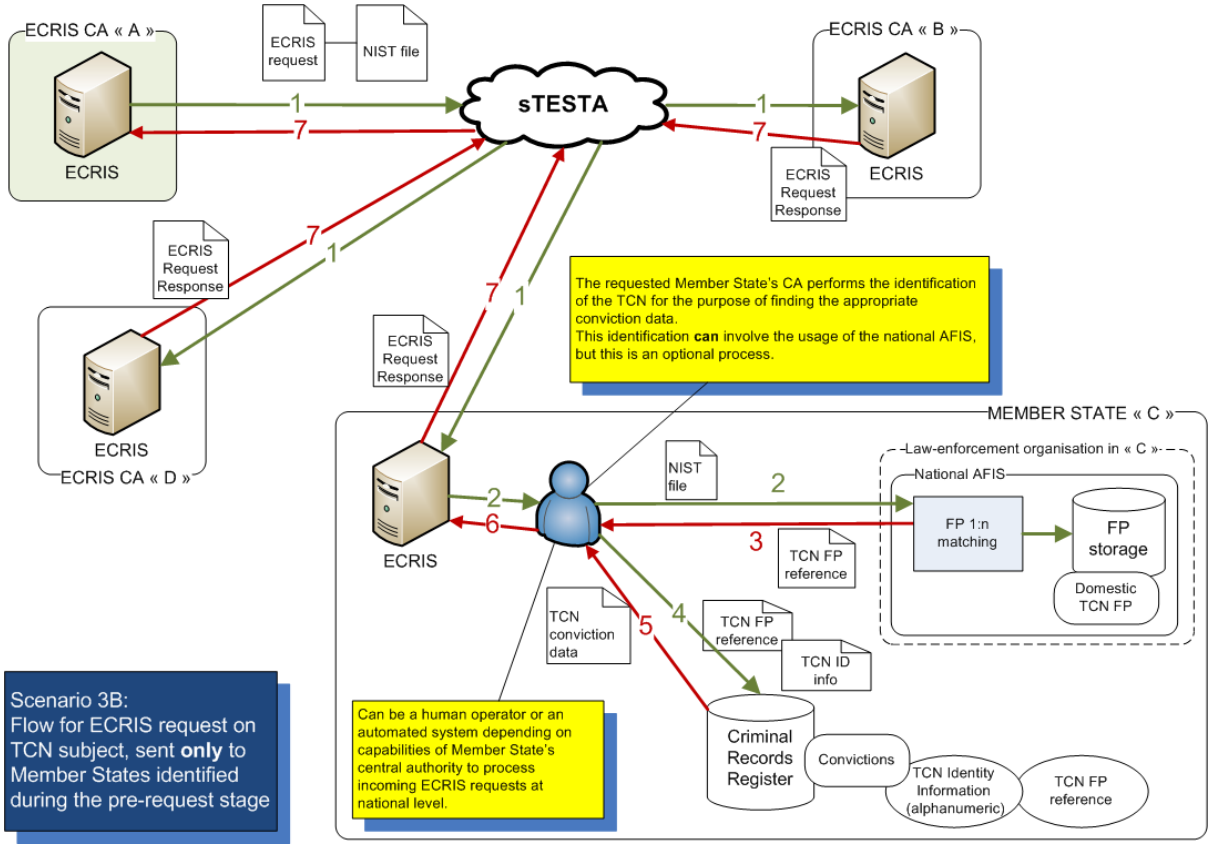
Figure 34 Process for central and local "hit/no hit" search in Scenario 3B



6.3.2.5 Process: ECRIS requests

The handling of the ECRIS request is similar to Scenario 3A, with the addition that the requested Member State that has opted for Scenario 3B can further use the national AFIS for performing additional manual verification of the fingerprints received. This facilitates the identification of the TCN subject in view of extracting the appropriate conviction information from the criminal records register. Figure 35 illustrates the described process for Scenario 3B.

Figure 35 Process for ECRIS request in Scenario 3B



6.4 Description of Scenario 4: central ECRIS TCN system, fully centralised "hit/no hit" search

Scenario 4 is based on the implementation of a **central TCN system** holding both alphanumeric identity information and fingerprints**.** The scenario has the following key characteristics:

- A **central ECRIS TCN system** is put in place, under management of eu-LISA.
- Alphanumeric identity information of TCN convicted at national level is stored in the central **ECRIS TCN system**.
- **Pseudonymised fingerprints of TCN** convicted at national level **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 a **"hit/no hit" search in the central ECRIS TCN system** for identifying which other Member State(s) can be queried for information about these past convictions.

In this scenario, the Member States do not share any identity information regarding convicted TCN. The identity information is centralised in an EU-wide system dedicated to the purpose of ECRIS TCN and managed by eu-LISA. The alphanumeric identity information and the fingerprints will be kept separately, so that eu-LISA cannot match the identity information with the fingerprints.

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 local ECRIS TCN system. The local ECRIS TCN system pseudonymises the

fingerprints and transmits them together with the alphanumeric identity information 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 local ECRIS TCN system to find whether this TCN is known within the EU. The local ECRIS TCN system automatically contacts the central ECRIS TCN system in order to perform a matching process using both alphanumeric identity information and fingerprints to find which other Member States have information on past convictions. The CA then prepares an ECRIS request and sends it to the Member States found by the ECRIS TCN system.

Please note that this scenario does not necessarily require the pseudonymisation of the alphanumeric identity information. Therefore the descriptions made in the following sections do not include ma3tch processing of the alphanumeric data and it is also not included in the costing for this scenario.

6.4.1 Description of Scenario 4A

The following sections provide an overview of Scenario 4A and detail the main business processes regarding the exchange of information.

6.4.1.1 Overview

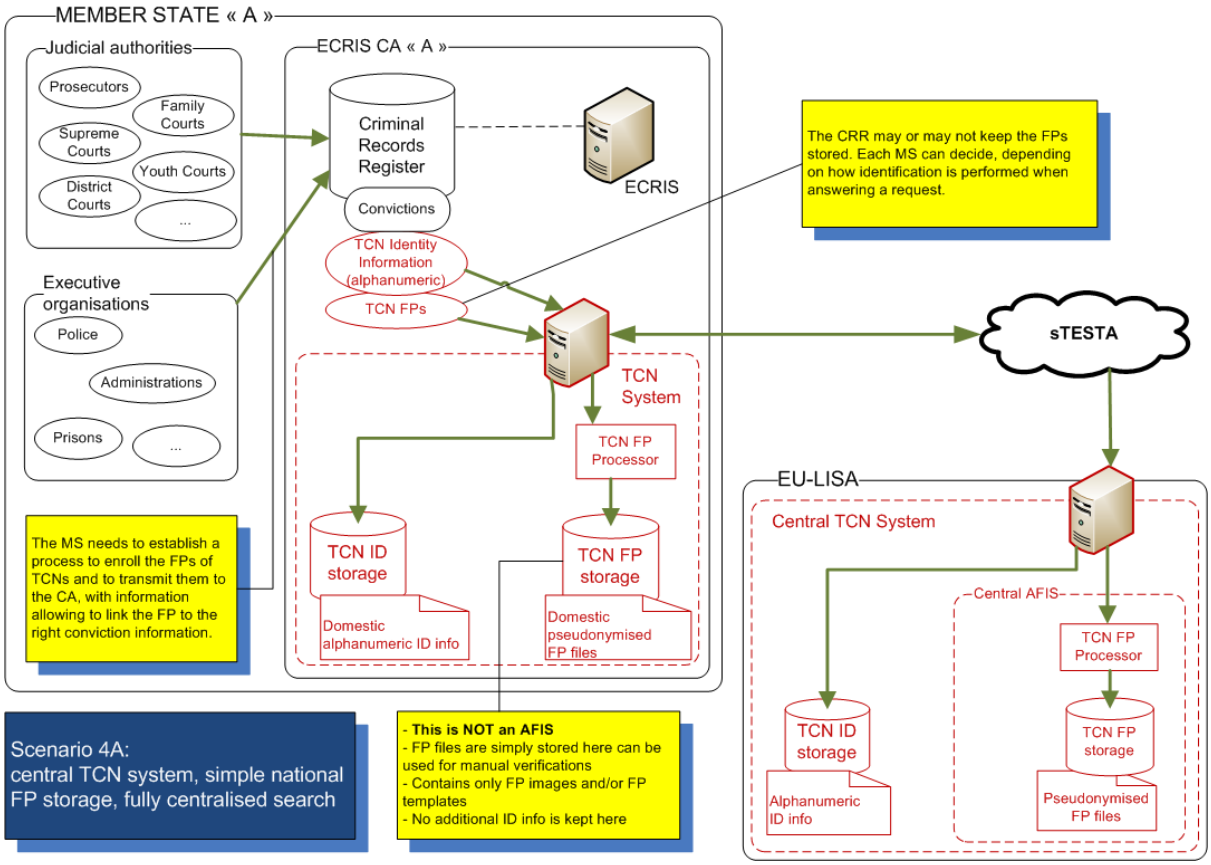
In this scenario the ECRIS TCN system at national level is composed of:

- The TCN FP storage: this part is not an AFIS but a technical component embedded within the ECRIS TCN system capable of pseudonymising and storing fingerprint files.
- The TCN ID storage for processing, storing and distributing alphanumeric identity information
- As in the previous scenarios the 2 components are completely separated and isolated in such a way that it is not possible to link the fingerprints kept in the TCN FP storage to any identity information kept in the TCN ID storage. The fingerprints are pseudonymised for protecting as much as possible the personal data.

At EU-level a full central ECRIS TCN system AFIS, dedicated to the purpose of ECRIS TCN exchanges, is set-up and managed by eu-LISA. This ECRIS TCN system is composed of an AFIS handling and storing fingerprints and a TCN ID storage keeping the alphanumeric identity information. The components in the central ECRIS TCN system are separated and isolated in such a way that fingerprints and alphanumeric identity information cannot be linked.

The national ECRIS TCN system is interconnected with the ECRIS system at national level and with the central ECRIS TCN system. Figure 36 illustrated the overview of Scenario 4A.

Figure 36 Overview of Scenario 4A

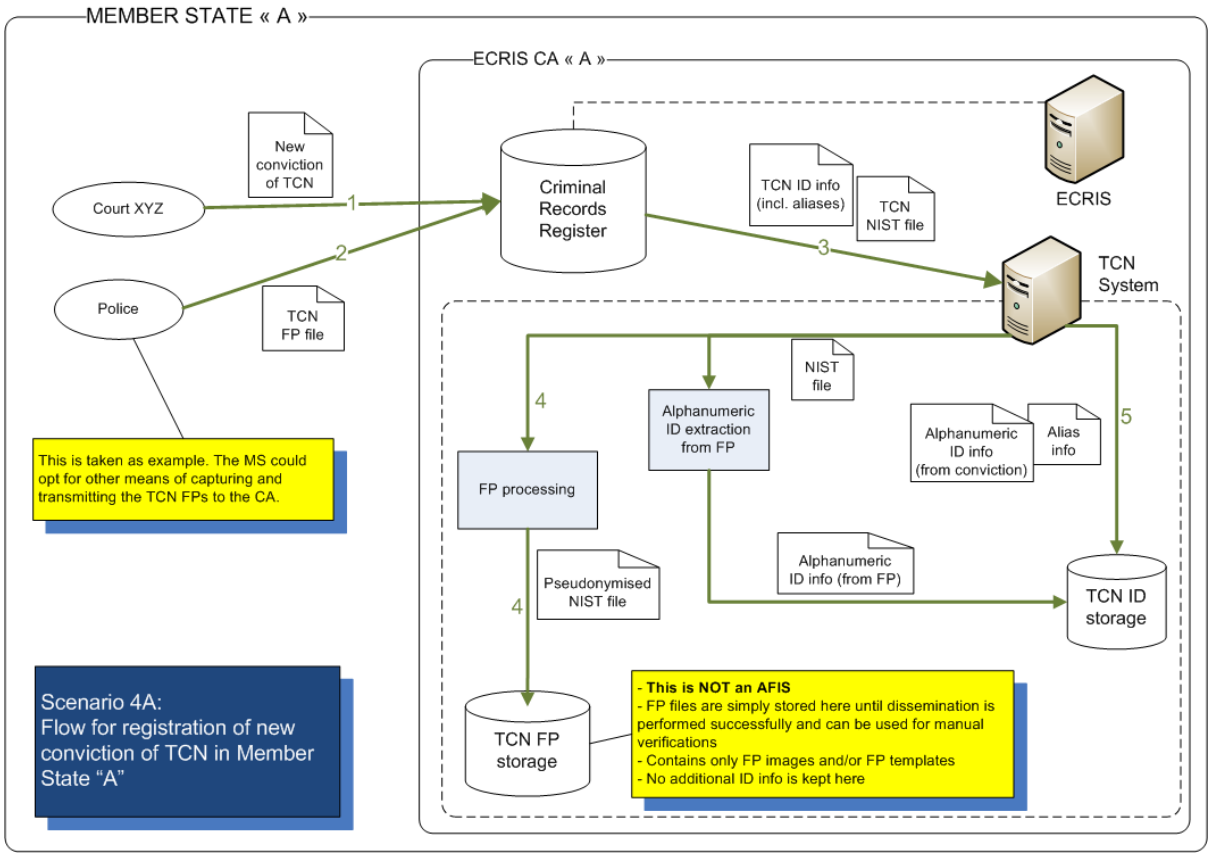


6.4.1.2 Process: new conviction of a TCN

This process works in the same way as for Scenario 3A.

The CA collects the conviction data and TCN fingerprints and feeds them into the national ECRIS TCN system, which pseudonymises the fingerprint data and stores them internally in the TCN ID storage and TCN FP storage. Figure 37 illustrates the described process for Scenario 4A.

Figure 37 Process for new conviction of a TCN in Scenario 4A

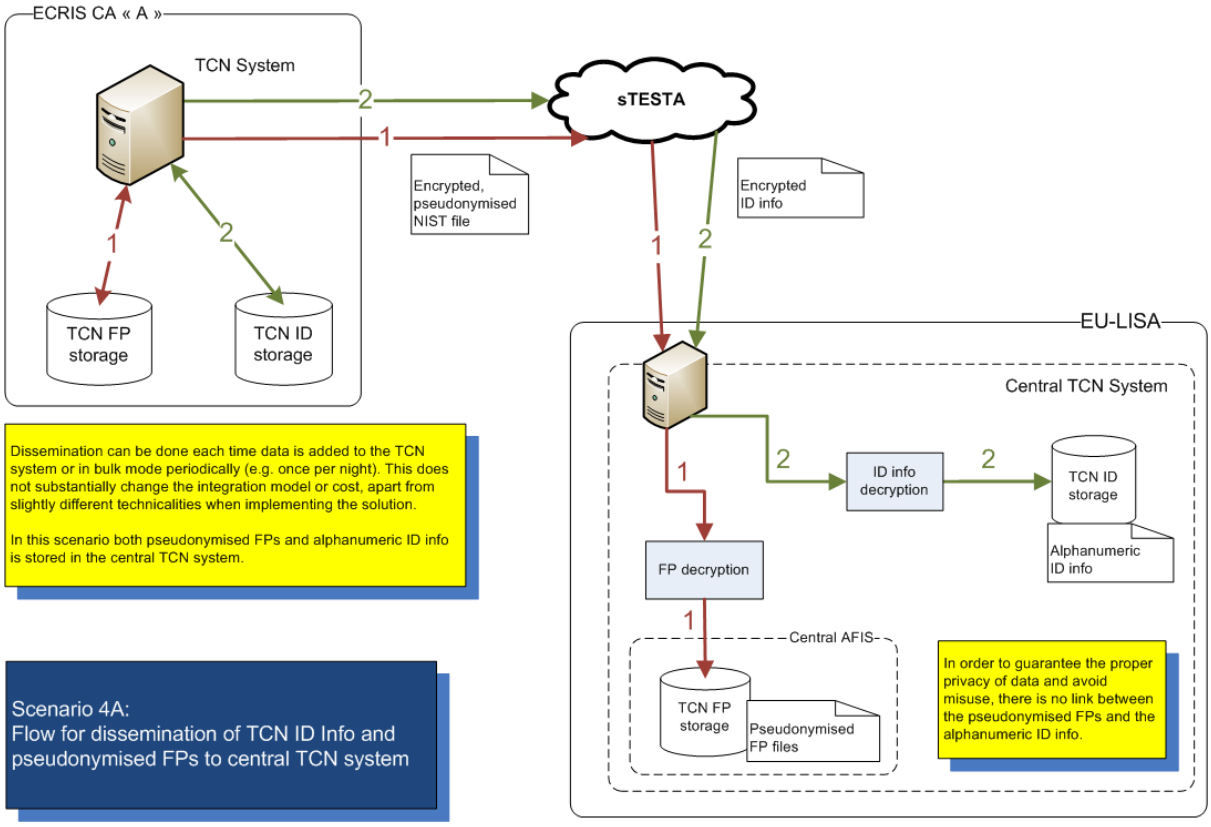


6.4.1.3 Process: dissemination of TCN identity information

The dissemination of TCN identity information differs from the previous scenarios. In this scenario, the national ECRIS TCN system simply encrypts the alphanumeric identity information and transmits it via sTESTA to the central ECRIS TCN system which stores it in its TCN ID storage. The fingerprints are pseudonymised and also transmitted to the central ECRIS TCN system via sTESTA, in a technically separate flow so as to avoid possibly linking the 2 streams of information. Here also the national ECRIS TCN system includes a unique technical reference and transmits it to the central ECRIS TCN system along with the pseudonymised fingerprints.

The central ECRIS TCN system then decrypts the received NIST file and stores it in such a way that they can be used for *one-to-many matching* with a maximum degree of accuracy. Figure 38 illustrates the described process for Scenario 4A.

Figure 38 Process for dissemination of TCN identity information in Scenario 4A



6.4.1.4 Process: central "hit/no hit" search for identifying Member States holding conviction data

In this *scenario* the "hit/no hit" search mechanism that aims at identifying the Member States holding information on past convictions of a given TCN subject relies only on the central ECRIS TCN system.

As for all other scenarios, this process also starts when an authorised authority within the Member State contacts the CA for requesting information on past convictions for a given TCN. The authority provides to the CA the identity of the TCN as well as the fingerprints. The CA then feeds all TCN information into the national ECRIS TCN system to trigger a "hit/ no hit" search.

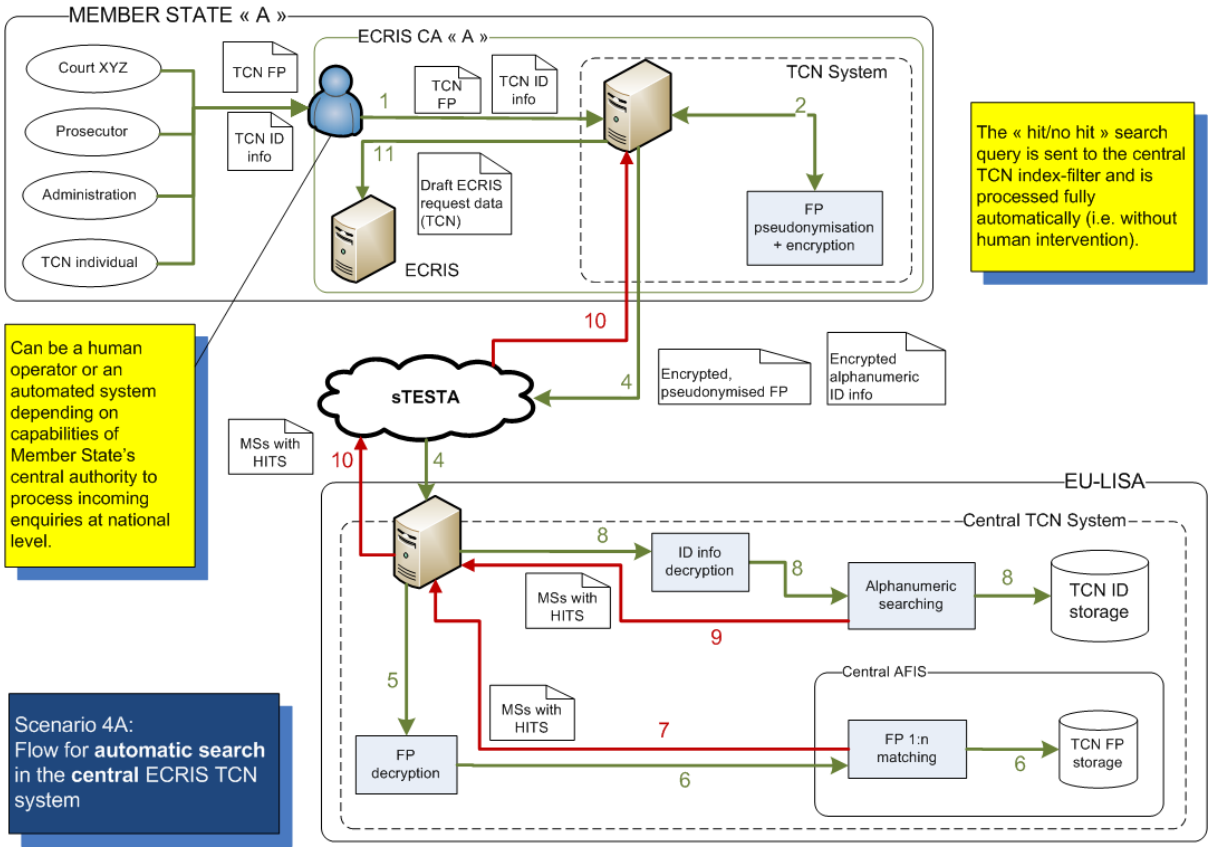
The ECRIS TCN system of the requesting CA automatically pseudonymises and encrypts the fingerprints file, encrypts the alphanumeric identity information and forwards the whole set of information to the central TCN system via the secured sTESTA network. The central ECRIS TCN system performs internally 2 tasks:

- It decrypts the fingerprints file and 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.
- It decrypts the alphanumeric identity information and performs a search to find corresponding matches in the TCN ID storage. This also results possibly in a list of Member States with hits.

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 requesting ECRIS TCN

system then automatically generates draft ECRIS requests targeting the Member States that were identified. Figure 39 illustrates the described process for Scenario 4A.

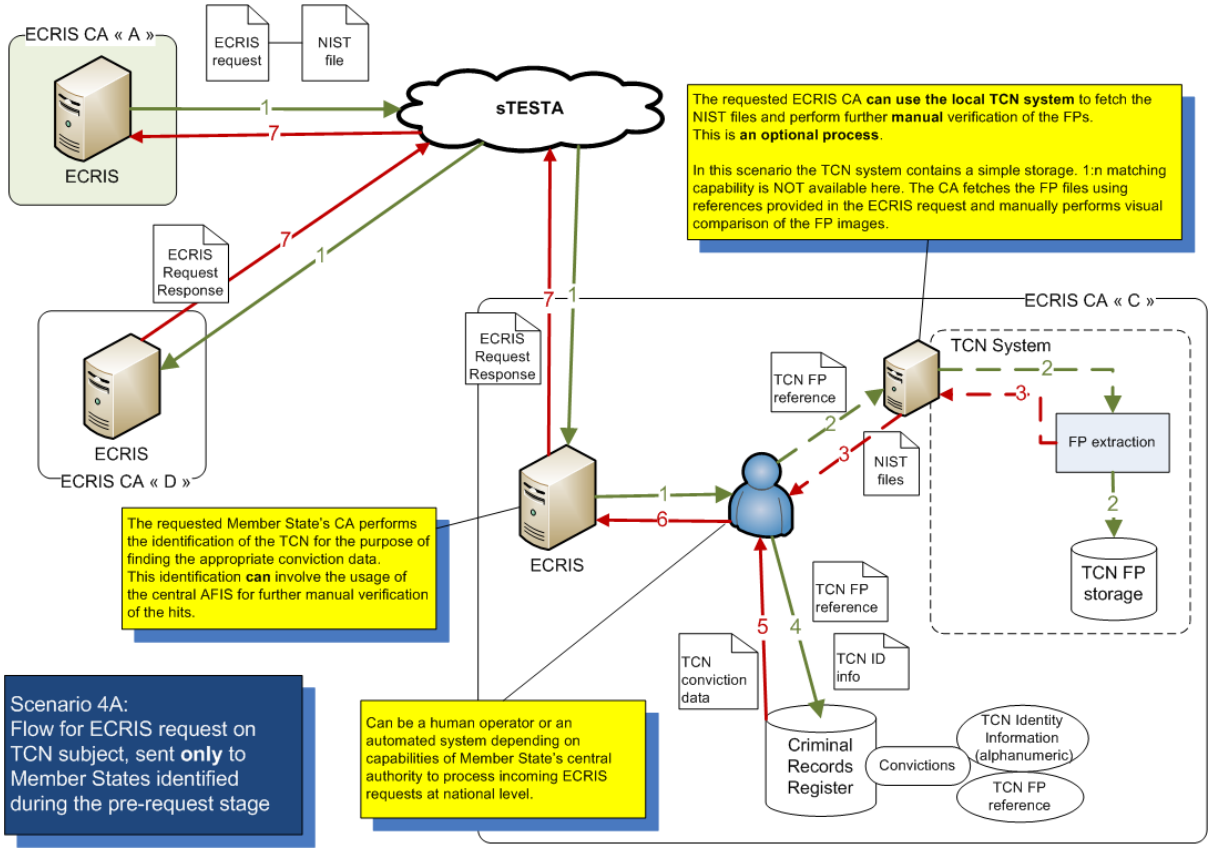
Figure 39 Process for central "hit/no hit" search in Scenario 4A



6.4.1.5 Process: ECRIS requests

The process of sending the ECRIS request to the Member State(s) identified during the previous "hit/no hit" search and to respond to them is identical to Scenario 3A. Similarly the requesting Member State is able to make use of the national ECRIS TCN system for extracting the fingerprints that caused the "hit" and performing a visual comparison with the fingerprints attached to the ECRIS request. Here also the TCN FP storage contained in the ECRIS TCN system is not a full AFIS and does not provide advanced functionality for facilitating this verification. Figure 40 illustrates the described process for Scenario 4A.

Figure 40 Process for ECRIS request in Scenario 4A



6.4.2 Description of Scenario 4B

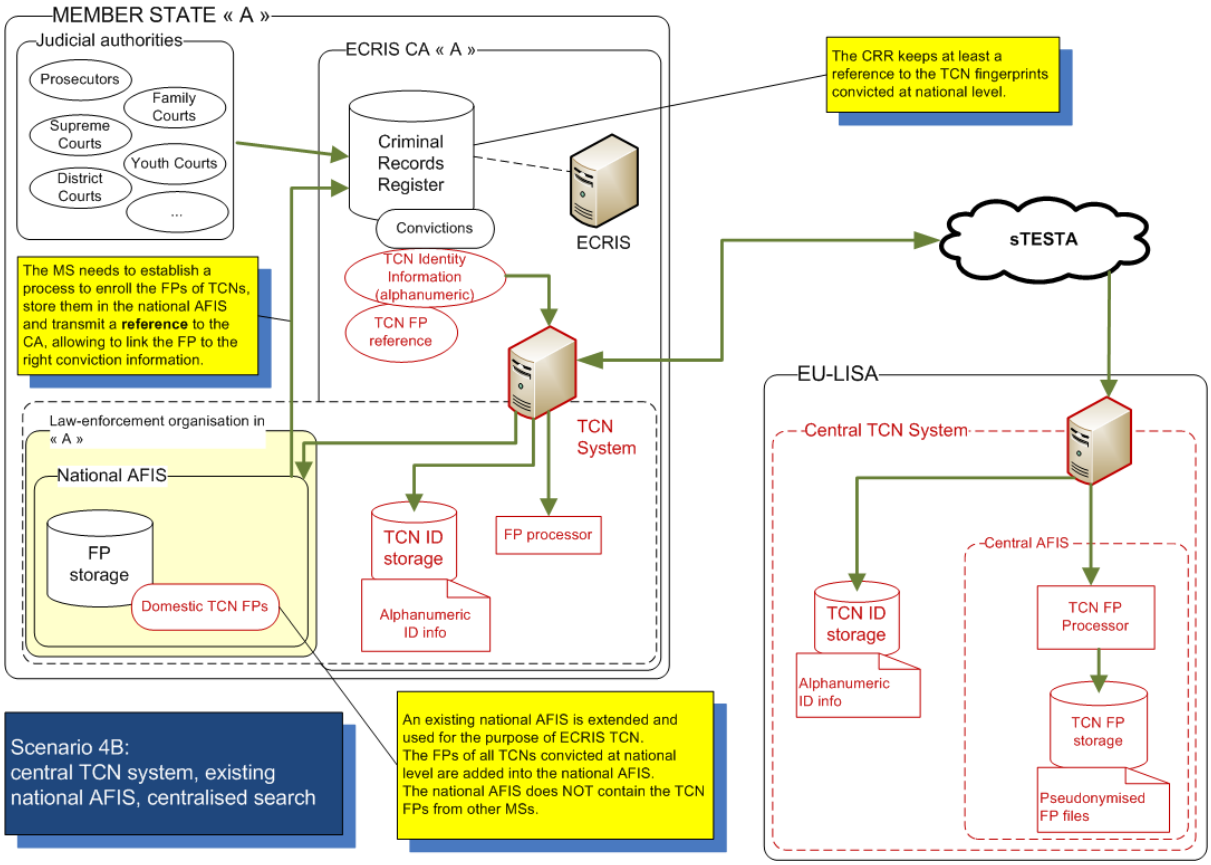
The following sections provide an overview of Scenario 4B and detail the main business processes regarding the exchange of information.

6.4.2.1 Overview

The main difference with Scenario 4A is that the national ECRIS TCN system does not contain its own dedicated fingerprint storage but links with a national AFIS that is extended and reused for the purpose of handling the TCN fingerprints.

Similar to previous scenarios, the national AFIS needs to be extended in such a way that it can include the fingerprints of TCN convicted at national level (labelled “domestic TCN fingerprints” in the diagram). Here also the national *AFIS* does not receive and store the pseudonymised fingerprints of TCN convicted by all other EU Member States as these are all stored in the central ECRIS TCN system managed by eu-LISA. The national ECRIS TCN system still contains the necessary technical components for storing and disseminating the alphanumeric identity information. Figure 41 illustrates the overview of Scenario 4B.

Figure 41 Overview of scenario4B

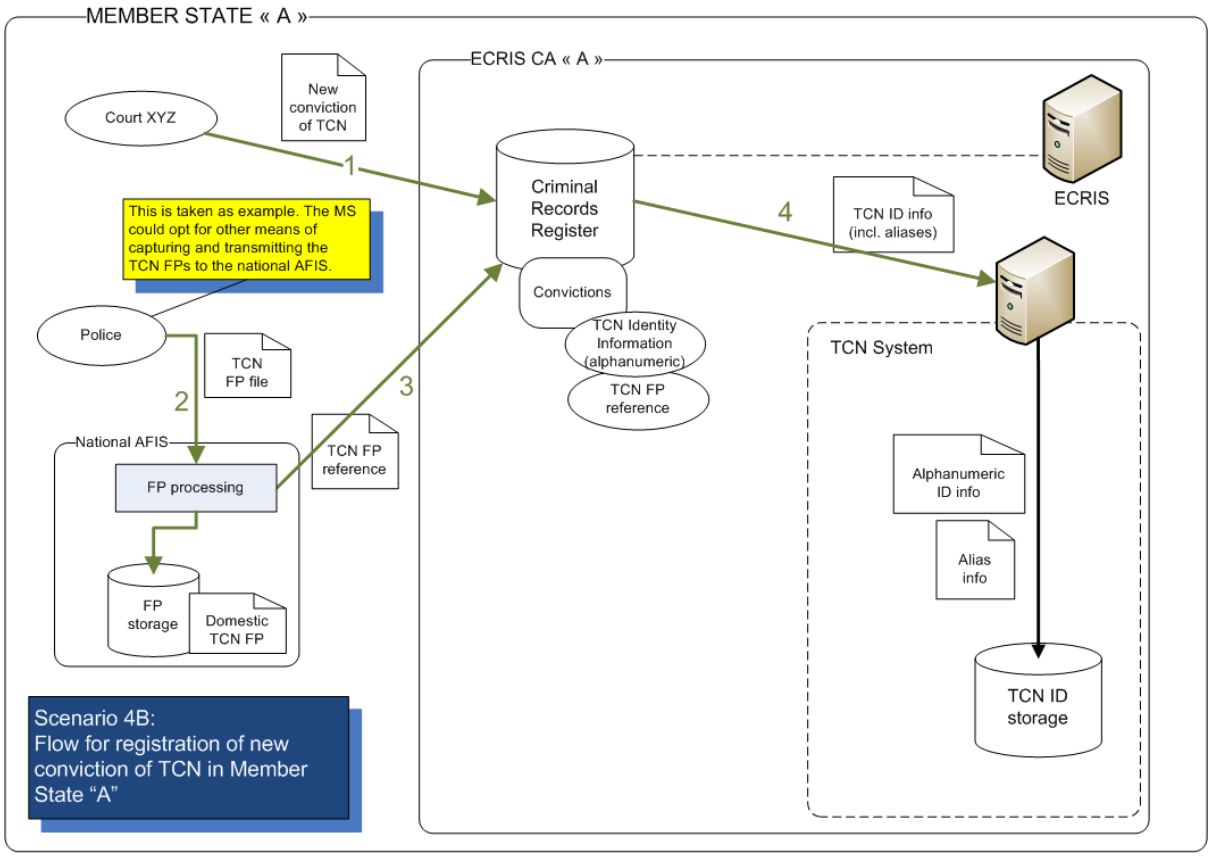


6.4.2.2 Process: new conviction of a TCN

This process works in the same way as for Scenario 3B.

The CA collects the conviction data and at least a technical reference to the TCN fingerprints. It enters the alphanumeric identity information into the national ECRIS TCN system which stores them internally in the TCN ID storage without further treatment. Figure 42 illustrates the described process for Scenario 4B.

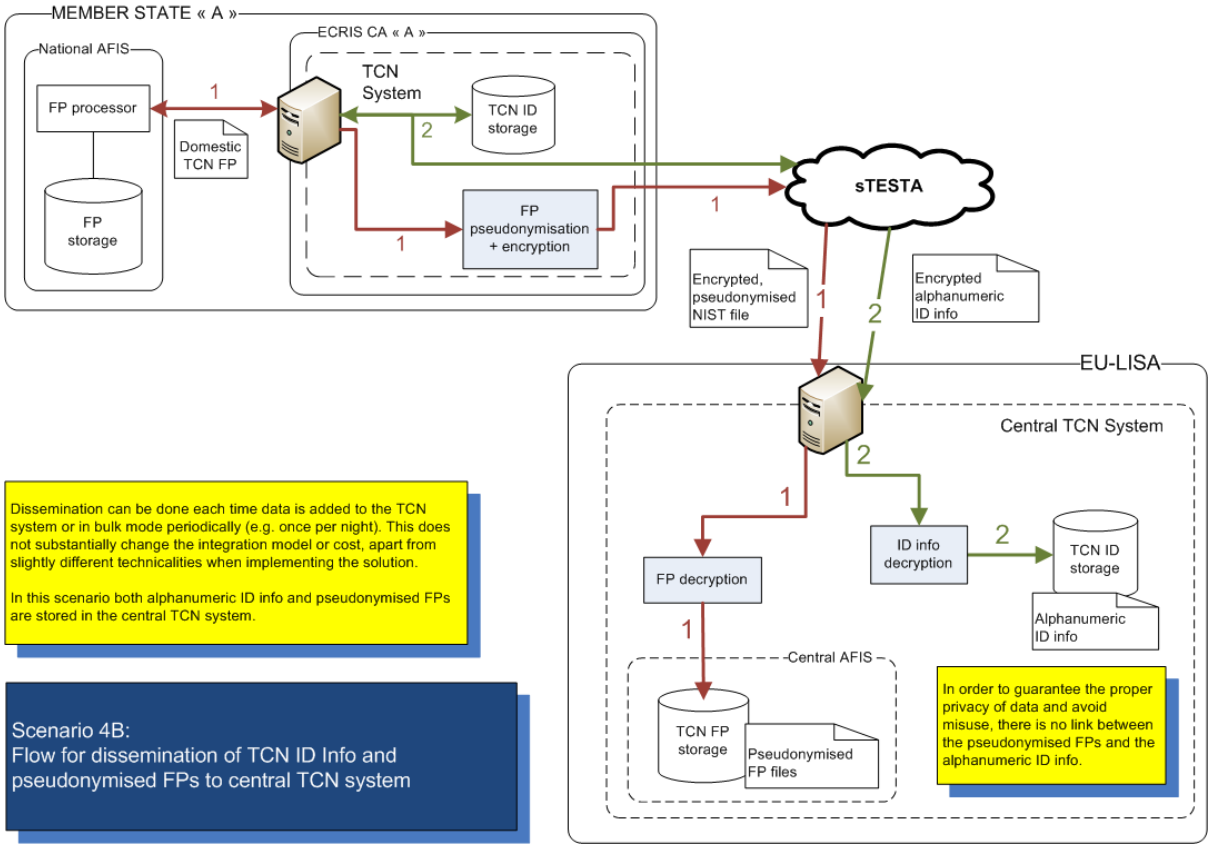
Figure 42 Process for new conviction of a TCN in Scenario 4B



6.4.2.3 Process: dissemination of TCN identity information

The dissemination of the TCN identity information works in the same way as in Scenario 4A with the exception that the national ECRIS TCN system needs to connect to the national AFIS in order to fetch the fingerprint files to be sent. The national ECRIS TCN system then transmits to the central ECRIS TCN system both the encrypted alphanumeric identity information and the encrypted, pseudonymised TCN fingerprint file. Figure 43 illustrates the described process for Scenario 4B.

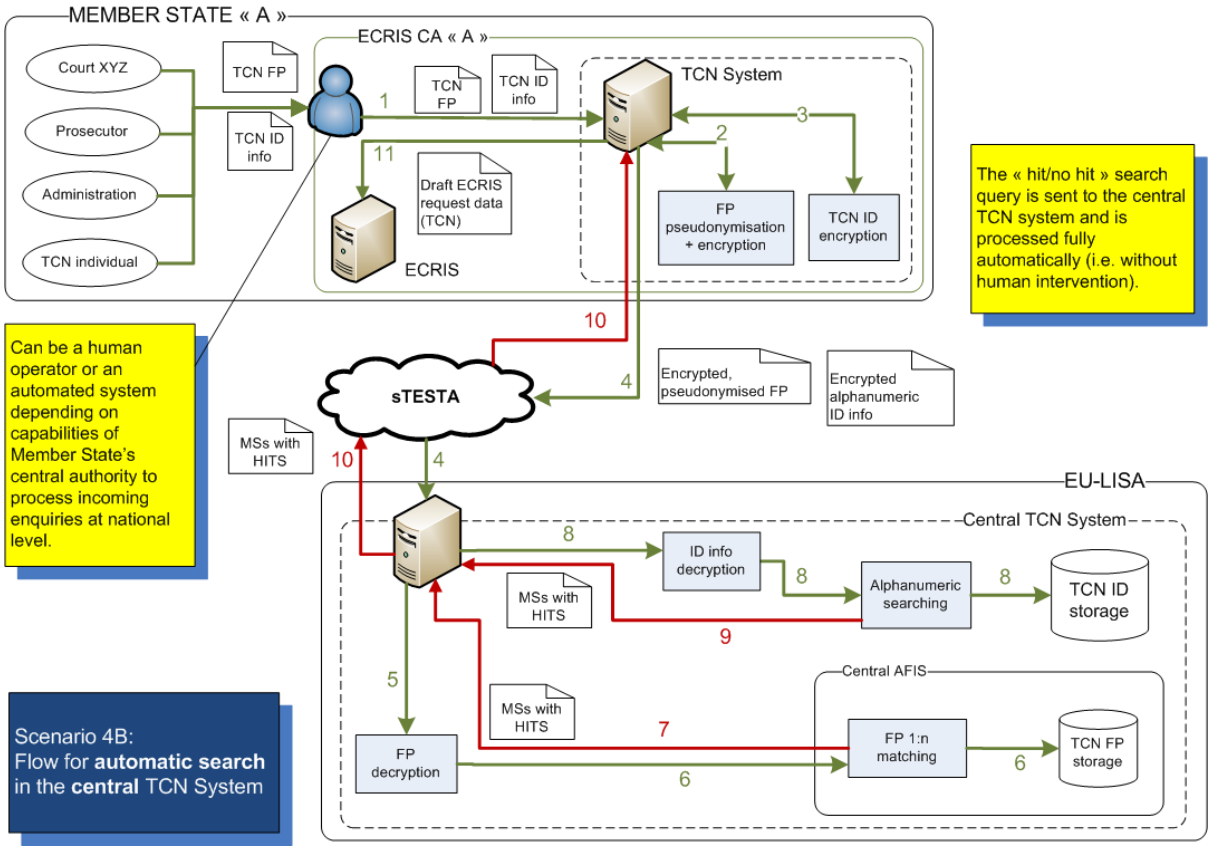
Figure 43 Process for dissemination of TCN identity information in Scenario 4B



6.4.2.4 Process: central "hit/no hit" search for identifying Member States holding conviction data

The "hit/no hit" search is identical to the one described in Scenario 4A. Here also the national ECRIS TCN system automatically encrypts the alphanumeric identity information and pseudonymised fingerprints of the TCN subject before triggering a "hit/no hit" search in the central ECRIS TCN system using the whole set of data. Figure 44 illustrates the described process for Scenario 4B.

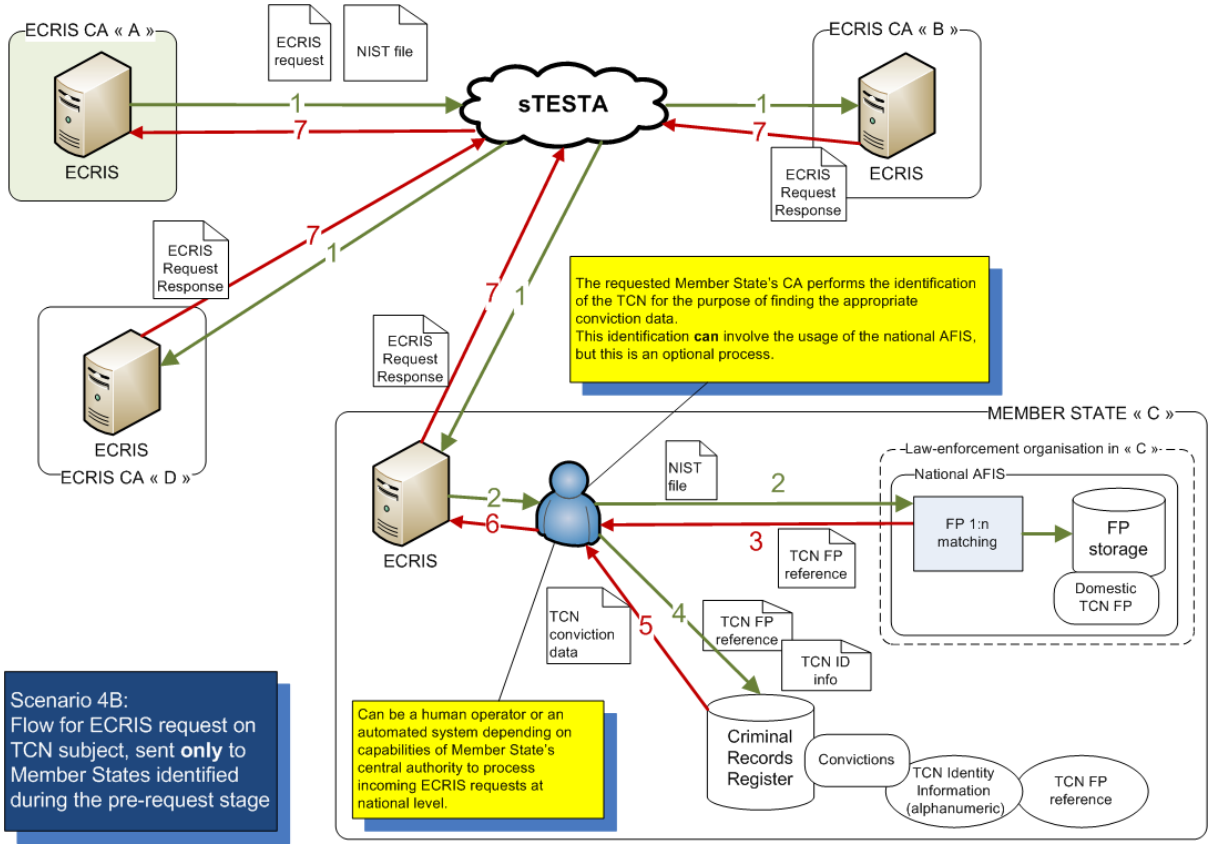
Figure 44 Process for central "hit/no hit" search in Scenario 4B



6.4.2.5 Process: ECRIS requests

The handling of the ECRIS request is similar to Scenario 4A, with the addition that the requested Member State that has opted for Scenario 4B can further use the national AFIS for performing additional manual verification of the fingerprints received. This facilitates the identification of the TCN subject in view of extracting the appropriate conviction information from the criminal records register. Figure 45 illustrates the described process for Scenario 4B.

Figure 45 Process for ECRIS request in Scenario 4B



6.5 Technical and operational impacts of the scenarios

This section provides a view on the technical and operational pros and cons on the implementation of the assessed scenarios. The pros and cons identified for each technical scenario can be perceived differently regarding their importance and priority, given the point of view of different stakeholders. Therefore, in this study we aim to present an objective view on the technical and operational aspects of each scenario as a conclusion.

Scenario 1: decentralised ECRIS TCN system, sharing of fingerprints and local "hit/no hit" search

PROS:

- In this scenario, each national ECRIS TCN system is technically independent from the installations of other Member States. In case one of the ECRIS TCN systems is unavailable (e.g. for maintenance purposes), it does not affect the other ECRIS TCN systems which can still operate.
- Each Member State manages its own ECRIS TCN system installation without technical dependencies with the other ECRIS TCN systems. In particular, each Member State has thus the possibility to select different AFIS vendors and IT subcontractors, depending on their procurement processes and particularities (provided that the IT solution meets the technical specifications defined for ECRIS TCN).
- As in ECRIS, this scenario allows Member States to progressively interconnect the ECRIS TCN systems, independently from a central entity. This provides additional flexibility for practical bilateral agreements between Member States.

- The capacity to execute one-to-many matching operations of the embedded AFIS can be tailored to the need of each Member State. This is due to the fact that each "hit/no hit" search is executed at national level. The number of search operations thus directly depends on how many requests relating to TCN the Member State needs to issue.
- In both variants A and B the central authority can rely on the additional capabilities of the AFIS system (either the dedicated AFIS embedded in the ECRIS TCN system in Scenario 1A or the national AFIS reused in Scenario 1B). The central authority of the Member States thus has additional IT features and tools available at national level for performing additional verification and identification tasks when replying to ECRIS requests.
- In Scenario 1A, the dedicated AFIS is operated by the central authority. This means that all the tools required by ECRIS are managed and operated by the same authority, whereas in Scenario 1B, the national AFIS is usually managed and operated outside of the central authority.

CONS:

- The identity information, including fingerprints and alphanumeric data, is replicated 28 times. This is technically more complex as it requires a continuous synchronisation between all Member States. This also makes it more difficult, from a technical and operational point of view, to solve discrepancies resulting from break-downs and interruptions. It is also less attractive from a data protection point of view.
- As TCN fingerprints are replicated in all Member States, all Member States need to invest in an AFIS solution sized for the storage of a large amount of data, independent of the size of the Member State and of its percentage of usage of the ECRIS TCN system.
- The dissemination of identity information is more complex as it requires 54 separate flows for each convicted TCN (one flow for the fingerprints and a distinct one for the alphanumeric data – spread over 27 Member States). Especially for Member States handing down large amounts of convictions on TCN, this can create a significant additional operational burden as the probability of failures increases.
- The dissemination process requires that each Member State establishes and maintains 27 secured interconnections with other Member States. The management, follow-up and maintenance of these interconnections also create an additional operational workload. This is however moderated by the fact that such operational processes are already in place for ECRIS.

Scenario 2: decentralised ECRIS TCN system, no sharing of fingerprints and distributed "hit/no hit" search

PROS:

- Each Member State manages its own ECRIS TCN system installation, without technical interdependencies with the other Member States. In particular, each Member State thus has the possibility to select different AFIS vendors and IT subcontractors, depending on their procurement processes and particularities (provided that the IT solution meets the technical specifications defined for ECRIS TCN).
- Since the fingerprint data are not copied to all Member States, this solution is more data protection friendly.

- As in ECRIS, this scenario allows Member States to progressively establish the interconnections between their ECRIS TCN systems, independently from an EU-institution. This provides additional flexibility for practical bilateral agreements between Member States.
- The storage capacity of the AFIS embedded in the ECRIS TCN system can be tailored to the needs of each Member State as it contains only the fingerprints of TCN convicted at national level. Member States handing down small amounts of convictions against TCN proportionately need less storage capacity than “high” producers.
- In both variants A and B, the central authority is able to rely on the additional capabilities of the AFIS system (either the dedicated AFIS embedded in the ECRIS TCN system in Scenario 2A or the national AFIS reused for ECRIS TCN in Scenario 2B). The central authority of the Member States has thus additional IT features and tools available at national level for performing additional verification and identification tasks, when replying to ECRIS requests concerning TCN.

CONS:

- In this scenario, the “hit/no hit” search queries are distributed across the ECRIS TCN systems of the 27 Member States. This implies that it multiplies the points of possible failure, which increases the probability of disrupted working. Also, in case one or several ECRIS TCN systems are unavailable, it interrupts the search, increases the time to verify whether there is a "hit", leading to a risk to miss a “hit”, and subsequently to miss past convictions handed down against the TCN.
- The dissemination process requires that each Member State establishes and maintains 27 secured connections with all other Member States. The management, follow-up and maintenance of these connections also create an additional operational workload. This is however moderated by the fact that such operational processes are already in place for ECRIS and that the dissemination only concerns the alphanumeric identity data without fingerprints.
- The “hit/no hit” search being systematically distributed to all other 27 Member States implies that all Member States will face large amounts of “hit/no hit” queries. This implies that the AFIS used by all the Member States need to have the highest capacity in terms of one-to-many matching of fingerprints. This will be particularly burdensome for Member States currently operating smaller AFIS systems.
- The distributed “hit/ no hit” search query is more complex from a technical and operational point of view as the requestor needs to wait for and consolidate the 27 replies of all partner Member States. This adds an additional operational burden for the Member States as it increases the probability of failures.

Scenario 3 central AFIS, sharing of alphanumeric data, "hit/no hit" search at central and local level

PROS:

- Each Member State manages its own ECRIS TCN system installation, without technical interdependencies with the other Member States. In particular, each Member State thus has the possibility to select different AFIS vendors and IT subcontractors, depending on their procurement processes and particularities (provided that the IT solution meets the technical specifications defined for ECRIS TCN). Even Member States that would choose Scenario 3A do not need to purchase an AFIS platform, which is in general a complex and expensive IT system.
- The capacity of the fingerprint storage embedded in the ECRIS TCN system can be tailored to the needs of each Member State, as it contains only the fingerprints of TCN convicted at national level. Member States handing down small amounts of convictions against TCN proportionately need less storage capacity than "high" producers.
- All "hit/no hit" searches using fingerprints are directed to the central AFIS. This implies that the component handling the TCN fingerprints within the ECRIS TCN system installed at national level does not need to have the processing capacity for executing large numbers of one-to-many matching operations.
- In this scenario it is possible for the central AFIS to provide additional features to the human operators of the central authorities of Member States. New features and tools of common interest to many Member States could thus be added in the future. As an example, it would be possible to provide remote access to the User Interface of the central AFIS. Operators of the requested central authority would then be able to perform remote one-to-many matching in the central AFIS, using the fingerprints received in the ECRIS request, and visual comparison and verification. Please note that these additional features are not included in the calculations of volume and in cost assessments.

CONS

- The risk of being locked to one specific vendor is higher due to the fact that the AFIS managed by eu-LISA would centralise the fingerprints of all convicted TCN. Please note that this risk can be mitigated when defining the detailed technical specifications for the central AFIS to be set-up. In particular, these specifications should prefer, when technically possible, the usage of international standards, formats and processing techniques so as to avoid reliance on vendor-specific characteristics as much as possible.
- The whole ECRIS TCN system relies on a single central AFIS, which creates a single point of failure. In case the central AFIS is unavailable, Member States cannot perform "hit/no hit" queries using fingerprints. The ECRIS TCN is however not completely blocked as it can still be used with alphanumeric identity data. This risk could be mitigated through providing redundant solutions.
- The dissemination process requires that each Member State establishes and maintains 28 secured connections: 27 connections with all other Member States for sharing the alphanumeric identity data and one connection to the central AFIS. The management, follow-up and maintenance of these connections also create an additional operational workload. This is however balanced by the fact that such operational processes are already in place for ECRIS.
- The dissemination of TCN identity is complex as it requires systematic data exchanges with 2 different systems: the ECRIS TCN systems of all 27 other Member States and the central AFIS (28

data flows for each TCN identity). However, the dissemination process for fingerprints is relatively simple in this option, since fingerprint data only need to be sent to one central point at eu-LISA.

- Especially for Member States handing down large amounts of convictions on TCN this can create a significant additional operational burden as the probability of failures increases. This makes it also more difficult, from a technical and operational point of view, to solve discrepancies resulting from break-downs and interruptions.
- The AFIS managed by eu-LISA would centralise the fingerprints of all TCN convicted throughout the EU and needs to process "hit/no hit" searches for all Member States. It therefore needs to have storage capacity for large amounts of fingerprints (equal to the storage capacity required by scenario 1) but combined with the capacity of processing large numbers of the most complex processing operations per day (in particular processing of incoming fingerprints for indexing and storage, combined with the one-to-many matching operations at the same time).
- Additional data protection provisions will need to be established for the central system.

Scenario 4 central ECRIS TCN system, fully centralised "hit/no hit" search

PROS

- Each Member State manages its own ECRIS TCN system installation, without technical interdependencies with the other Member States. In particular, each Member State thus has the possibility to select different AFIS vendors and IT subcontractors, depending on their procurement processes and particularities (provided that the IT solution meets the technical specifications defined for ECRIS TCN). Even Member States that would choose Scenario 4A do not need to purchase an AFIS platform, which is in general a complex and costly IT system.
- The capacity of the fingerprint storage embedded in the ECRIS TCN system can be tailored to the needs of each Member State as it contains only the fingerprints of TCN convicted at national level. Member States handing down small amounts of convictions against TCN proportionately need less storage capacity than "high" producers.
- All "hit/no hit" searches are directed to the central AFIS. This implies that the components handling the TCN fingerprints and alphanumeric data within the ECRIS TCN system installed at national level do not need to include capacity for executing large numbers of one-to-many matching operations.
- Compared with the previous scenarios, the dissemination of TCN identity information is easier in this case because all identity information is transmitted only to the central ECRIS TCN system.
- The dissemination process and "hit/no hit" searches only need a connection between the national ECRIS TCN system and the central ECRIS TCN system. There is thus no need for Member States to establish and maintain many additional secured interconnections with other Member States.
- In this scenario it is possible for the central AFIS to provide additional features to the human operators of the central authorities of Member States. New features and tools of common interest to many Member States could thus be added in the future. As an example, it would be possible to provide remote access to the User Interface of the central AFIS. Operators of the requested central authority would then be able to perform remote one-to-many matching in the central AFIS, using the fingerprints received in the ECRIS request, and visual comparison and verification. Please note here that these additional features are not included in the calculations of volume and in cost assessments.

CONS

- The risk of being locked to one specific vendor is higher due to the fact that the AFIS managed by eu-LISA would centralise the fingerprints of all convicted TCN. Please note that this risk can be mitigated when defining the detailed technical specifications for the central AFIS to be set-up. In particular these specifications should prefer, when technically possible, the usage of international standards, formats and processing techniques so as to avoid reliance on vendor-specific characteristics as much as possible.
- The whole ECRIS TCN system relies on a single central system, which creates a single point of failure. In case the central ECRIS TCN system is unavailable, Member States cannot perform "hit/no hit" searches at all. This implies that the central ECRIS TCN system needs to be operated and managed in a way to ensure a high level of availability and short recovery periods in case of break-down. This risk could also be mitigated through providing redundant solutions.
- The AFIS managed by eu-LISA would centralise the fingerprints of all TCN convicted throughout the EU and needs to process "hit/no hit" searches for all Member States. It therefore needs to have storage capacity for large amounts of fingerprints (equal to the storage capacity required by scenario 1) but combined with the capacity of processing large numbers of the most complex processing operations per day (in particular processing of incoming fingerprints for indexing and storage, combined with the one-to-many matching operations at the same time)..

In addition to the pros and cons presented above, it is also interesting to point out the main differences between variants A and B within each scenario:

- Variant A is usually more straightforward, in terms of management and operation, as all the components used for ECRIS TCN are under the sole responsibility of the central authority (in the majority of Member States within the Ministry of Justice). This makes it more straightforward to take budgetary and managerial decisions (e.g. hiring additional operators or fingerprint experts for the needs of ECRIS TCN, upgrading the capacity of the ECRIS TCN system, etc.).
- Variant B, in many Member States, will require establishing close cooperation between the central authority responsible for ECRIS and the competent authority responsible for the management and operation of the national AFIS. Frequently, the authority managing the national AFIS is under the responsibility of another Ministry than the one responsible for ECRIS, which can make it more difficult to establish operational and practical working processes. However, variant B has the advantage that the central authority can benefit from the features and content provided by the existing national AFIS, as well as the proven experience of specialised experts, already involved with fingerprints for many years.

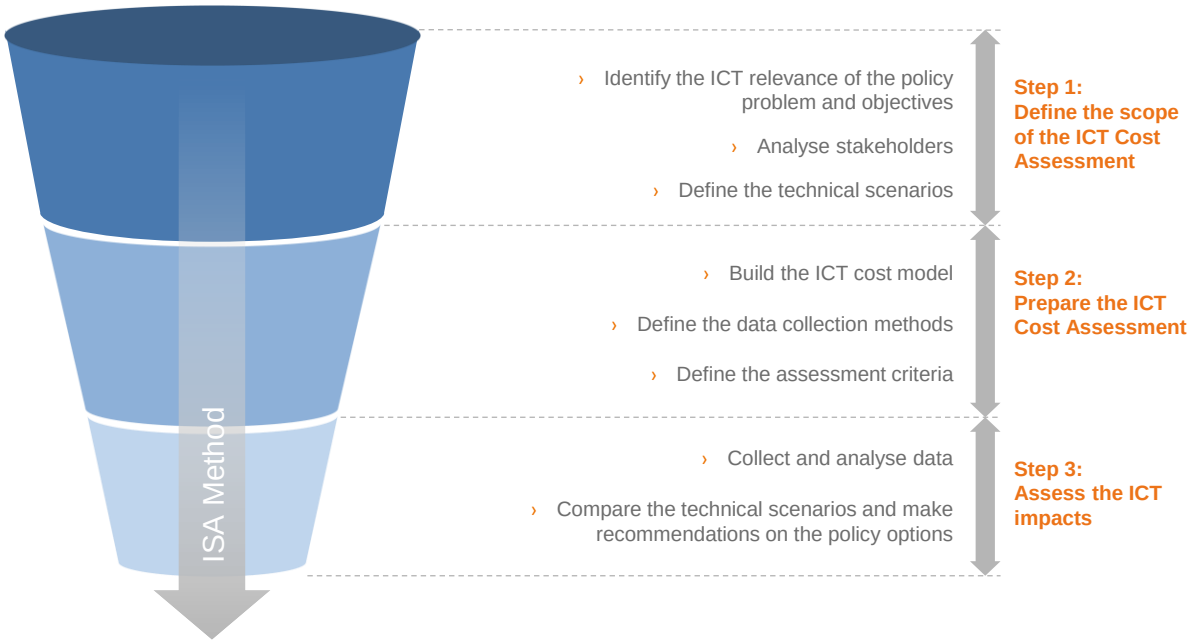
7 Costs associated with the technical scenarios

This section presents the costs associated with the identified technical scenarios to implement an ECRIS TCN system with the inclusion of pseudonymised fingerprints. The section details the methodology used to conduct this ICT Costs Assessment, lists all general assumptions used for the cost estimations, provides an overview and comparison of each technical scenario in terms of cost elements and administrative costs, and concludes on the least-cost technical scenario to implement an ECRIS TCN system with the inclusion of pseudonymised fingerprints.

7.1 Methodology

The ICT Assessment of the impacts of the legislative proposal for ECRIS TCN exchanges with the inclusion of pseudonymised fingerprints follows a set of logical steps. They 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 methodology followed for the ICT Cost Assessment comprises three steps, namely: Step I: Define the scope of the ICT Cost Assessment; Step II: Prepare the ICT Cost Assessment; Step III: Assess the ICT impacts. This methodology presented in Figure 46 below was developed by ISA Programme[42] and is referred in the Better Regulation Guidelines from the Commission[43].

Figure 46 ICT Cost Assessment Overall Approach



[42] The ISA Method for Assessing ICT Implications of EU Legislation is applied to the assessment of impacts approach, 2015. Available at http://ec.europa.eu/isa/documents/actions/ks-sc9-d04-03-ict-assessment-method_v5.00.pdf.
[43] Better Regulation Guidelines [COM (2015)205 final] European Commission, 19.05.2015

7.1.1 Step I: Define the scope of the ICT Cost Assessment

The first step of the methodology is to define the scope of the ICT Cost Assessment of the legislative proposal for an ECRIS TCN system.

For this purpose, the following actions were performed:

1. Identification of the ICT relevance of the policy problem and objectives (section 7.1.1.1);
2. Identification of the stakeholders affected by each technical scenario (section 7.1.1.2); and
3. Definition of the technical scenarios (section 7.1.1.3).

7.1.1.1 Identification of the ICT relevance of the policy problem and objectives

The first step of the ICT Cost Assessment methodology is to identify the ICT relevance of the policy problem and objectives of the study. In this study, this step is performed as the investigation of the feasibility of including pseudonymised fingerprints in ECRIS TCN exchanges. This is presented in detail in sections 1, 2, 3, 4, and 5.

7.1.1.2 Stakeholder analysis

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

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

Table 4 provides a summary of the different stakeholder groups affected by the technical scenarios defined in section 6.

Table 4 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	• One unit from DG JUST, • eu-LISA representatives	• **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 the ICT Cost Assessment lead DG (DG JUST). This group will be affected by all of the assessed technical scenarios, as, in each case, the European Commission will be involved in developing the technical specifications for an ECRIS TCN exchanges, update of the ECRIS technical specifications and development of ECRIS Reference Implementation. Detailed mapping of each cost element affecting the European Commission stakeholder group is presented in the following sections. • **eu-LISA** - 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 in case one of the following scenarios is chosen: 3A, 3B, 4A, or 4B where eu-LISA would be responsible for setting up a central AFIS system.

Stakeholder Group code (SG)	Stakeholder Group Name (SGN)	Size of the stakeholder group	Description of the stakeholder group
SG02	National Competent Authorities (NCAs)	• 28 ECRIS Member State Competent Authorities	• **NCAs** – 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. National Competent Authorities will be affected by all Scenarios. Detailed mapping of each cost element affecting the National Competent Authorities stakeholder group is presented in the following sections.

7.1.1.3 Definition of the technical scenarios

Several technical scenarios and variants for the implementation of an ECRIS TCN exchanges with the inclusion of fingerprints have been identified. Following that, the technical scenarios were narrowed down to eight possible technical scenarios considered so far as the most realistic and feasible to enable the exchange of data on convicted TCN among Member States. The objective of this part of the study is to evaluate the costs related to the eight technical scenarios qualified to implement the ECRIS TCN exchanges with the inclusion of pseudonymised fingerprints. The eight scenarios are described in detail in section 6.

7.1.2 Step II: Prepare the ICT Cost Assessment

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

- Building an ICT cost model for each technical scenario (section 7.1.2.1); and
- Defining the data collection methods to be applied (section 7.1.2.2).

7.1.2.1 Building the ICT cost model

The Better Regulation Guidelines[43] and Better Regulation Toolbox[44] set a list of regulatory costs and benefits[45] to be assessed in a full Impact Assessment study. In the scope of the current study, the ICT Cost Assessment focuses only on substantive compliance costs. The Better Regulation Toolbox defines substantive compliance costs as:

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 according to the ICT cost categories specified in the Value Assessment Tool (VAST[46]) guidelines of the European Commission which are:

[44] 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.
[45] This ICT assessment is only focused on the costs related to the implementation of the technical scenarios; regulatory benefits are out of the scope of this assessment.
[46] Value Assessment Tool guidelines, European Commission, Directorate-General for Informatics, 2010.

- Infrastructure costs were collected from all stakeholder groups in monetary values (Euros) and provide the total (anticipated) cost of:
    - Hardware costs – cost of servers, storage and processing capacity required to develop, support, operate and maintain the system.
    - Software costs – cost of software licences required to develop, support, operate and maintain the system.
- Development costs provide the total (anticipated) cost (human resources) for the development of the system (e.g. analysis and process re-engineering activity, coding activity, project management activity, test activity, configuration and change management activity, deployment activity). Development costs were collected from all stakeholder groups in monetary values (Euros);
- Maintenance costs provide the total (anticipated) cost (human resources) in person days per year to maintain the system (e.g. activities related to both corrective maintenance and evolving maintenance). Maintenance costs were collected from all stakeholder groups in monetary values (Euros);
- Support costs provide the total (anticipated) cost (human resources) per year to support the system, its users and end-users. Support costs were collected from all stakeholder groups in monetary values (Euros);
- Training costs are related to the costs of training three persons per Member State as users of the ECRIS TCN system. Training costs were computed using the labour rates for each Member State provided by Eurostat[47] for participants, and the labour rates of EU officials for trainers. Travel costs, accommodation, subsistence expenses for the participants and the trainers were also included in the calculations. The costs of transferring the knowledge on the ECRIS TCN system to more than three persons per Member State were not included in the cost estimates.

Important aspects of the calculation of the costs are presented in section 7.2.1 General assumptions.

The first step to building a cost model is breaking down each technical scenario 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 taking into account whether these costs are one-off or recurring (i.e. yearly recurring costs). 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 scenario is defined by the sum of each of its cost items.

Table 5 presents the technical scenarios decomposed into cost items and the cost categories associated to them. The table also shows whether one-off and recurring costs are associated to each cost item and cost category. Maintenance, support and training 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 'Set up of central AFIS system' (technical scenarios 3 and 4). 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 7.2 Cost assessment of the technical scenarios.

[47] Eurostat's structural earnings survey for occupation group ISCO 3 (Technicians and associate professionals), 2010.

Table 5 Technical scenarios and related cost items and ICT cost categories

Cost Category / Cost Items	Infrastructure		Development		Maintenance		Support		Training	
	One-off	Recurring	One-off	Recurring	One-off	Recurring	One-off	Recurring	One-off	Recurring
Scenario 1A										
Technical specification for an ECRIS TCN system			☑							
Update of the ECRIS technical specifications			☑							
Update of the ECRIS Reference Implementation			☑							
Development of the ECRIS TCN system Reference Implementation			☑			☑				
Setup of a dedicated AFIS system to support the ECRIS TCN system	☑		☑			☑		☑		
Set up the ECRIS TCN system for local query in the dedicated AFIS	☑		☑			☑		☑		
Training on the use of the fingerprints functionalities of ECRIS TCN system										☑
Scenario 1B										
Technical specification for an ECRIS TCN system			☑							
Update of the ECRIS technical specifications			☑							
Update of the ECRIS Reference Implementation			☑							
Development of the ECRIS TCN system Reference Implementation for local queries in a national AFIS			☑			☑				
Set up the ECRIS TCN system Reference Implementation for local query in the national AFIS	☑		☑			☑		☑		
Upgrade National AFIS	☑		☑							
Training on the use of the fingerprints functionalities of ECRIS TCN system										☑
Scenario 2A										
Technical specification for an ECRIS TCN system			☑							
Update of the ECRIS technical specifications			☑							
Update the ECRIS Reference Implementation			☑							
Development of the ECRIS TCN system Reference Implementation			☑			☑				
Setup of a dedicated AFIS system to support the ECRIS TCN system	☑		☑			☑		☑		
Set up the ECRIS TCN system for distributed “hit/no hit” search queries in dedicated AFIS	☑		☑			☑		☑		
Training on the use of the fingerprints functionalities of ECRIS TCN system										☑
Scenario 2B										
Technical specification for an ECRIS TCN system			☑							
Update of the ECRIS technical specifications			☑							
Update the ECRIS Reference Implementation			☑							
Development of the ECRIS TCN system Reference Implementation for distributed queries			☑			☑				
Set up the ECRIS TCN system for distributed “hit/no hit” search queries in national AFIS	☑		☑			☑		☑		
Upgrade National AFIS	☑		☑							
Training on the use of the fingerprints functionalities of ECRIS TCN system										☑

Cost Category / Cost Items	Infrastructure		Development		Maintenance		Support		Training	
	One-off	Recurring	One-off	Recurring	One-off	Recurring	One-off	Recurring	One-off	Recurring
Scenario 3A										
Technical specification for an ECRIS TCN system			☑							
Update of the ECRIS technical specifications			☑							
Update the ECRIS Reference Implementation			☑							
Development of the ECRIS TCN system Reference Implementation			☑			☑				
Set up of central AFIS system	☑	☑	☑			☑		☑		
Set up the ECRIS TCN system at national level for querying a central AFIS			☑			☑		☑		
Training on the use of the fingerprints functionalities of ECRIS TCN system										☑
Scenario 3B										
Technical specification for an ECRIS TCN system			☑							
Update of the ECRIS technical specifications			☑							
Update the ECRIS Reference Implementation			☑							
Development of the ECRIS TCN system Reference Implementation			☑			☑				
Set up of central AFIS system	☑	☑	☑			☑		☑		
Set up the ECRIS TCN system at national level for querying a central AFIS			☑			☑		☑		
Training on the use of the fingerprints functionalities of ECRIS TCN system										☑
Upgrade National AFIS for verification following a query in the central AFIS	☑		☑							
Scenario 4A										
Technical specification for an ECRIS TCN system			☑							
Update of the ECRIS technical specifications			☑							
Update the ECRIS Reference Implementation			☑							
Development of the ECRIS TCN system Reference Implementation			☑			☑				
Set up of central AFIS system	☑	☑	☑			☑		☑		
Set up the ECRIS TCN system at national level for querying a central AFIS			☑			☑		☑		
Training on the use of the fingerprints functionalities of ECRIS TCN system										☑
Scenario 4B										
Technical specification for an ECRIS TCN system			☑							
Update of the ECRIS technical specifications			☑							
Update the ECRIS Reference Implementation			☑							
Development of the ECRIS TCN system Reference Implementation			☑			☑				
Set up of central AFIS system	☑	☑	☑			☑		☑		
Set up the ECRIS TCN system at national level for querying a central AFIS			☑			☑		☑		
Training on the use of the fingerprints functionalities of ECRIS TCN system										☑
Upgrade National AFIS for verification following a query in the central AFIS	☑		☑							

7.1.2.2 Definition of the data collection methods

Based on the stakeholder analysis' results and on the specificities of each data collection method, the most appropriate data collection method(s) were defined (i.e. desk research, interviews, and workshop) in order to receive inputs on the ICT impacts of the technical scenarios for each stakeholder group, whether positive or negative, qualitative or quantitative.

Desk research is the instrument to screen and collect legal, policy, and technical information from the documentation available at national and EU level. It is mainly used in this study to assess the current situation on 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 ICT Cost Assessment, prior to using any other data collection method (e.g. interviews and workshop). The data collection covered legal texts, 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.

The project team conducted interviews with two AFIS vendors[48] to collect primary data relevant to the analysed technical scenarios. The interviews were supported by a structured questionnaire with a limited set of open questions. Primary data was also 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 exchanges. A workshop summary is presented in Annex 5. Additionally, primary data on the cost estimates were provided by ECRIS technical experts and by AFIS vendors. For data protection and business confidentiality purposes, the individual answers received from AFIS vendors and ECRIS experts are treaded anonymously, remained confidential, were only disclosed to the evaluation team and were used solely for research purposes.

Finally, in order to complement the information received from AFIS vendors and ECRIS technical specialists, cost estimates gathered from interviews conducted with eu-LISA and FIU.net in the course of the 2015 Assessment of ICT impacts on the legislative proposal for ECRIS TCN system[49] were extrapolated and used for the analysis of the technical scenarios.

7.1.3 Step III: Assess the ICT impacts

The third and last phase of the methodology aimed to conduct the ICT Cost Assessment. This phase consisted of data collection and data analysis following the methodology described in section 7.1 and comparison of the technical scenarios as presented section 7.3.

---

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

[49] 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. Available at: http://ec.europa.eu/justice/criminal/files/ecris_tcn_ict_impact_assessment_final_report_en.pdf

7.2 Cost assessment of the technical scenarios

This section presents the assessment of the technical scenarios for the inclusion of pseudonymised fingerprints in the ECRIS TCN system, including the main assumptions made to perform this assessment, and the detailed description of the cost items, comprising each technical scenario.

7.2.1 General assumptions

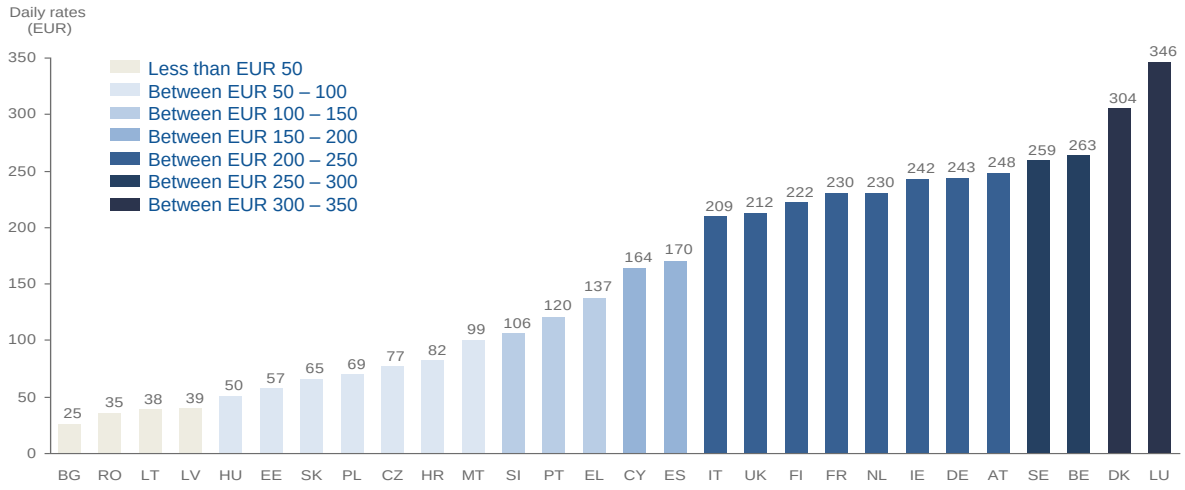
The ICT Cost Assessment of the technical scenarios takes into account several assumptions. Assumptions specific to each cost item are presented together with the detailed cost item description (sections 7.2.2 to 7.2.5). The following points describe general assumptions of the ICT Cost Assessment, which were applied to all technical scenarios:

- Number of TCN convictions – a relevant aspect for development of the ECRIS TCN system is the magnitude/size of the future database that needs to be established. The number of criminal records of TCN has a direct impact on the scalability of the system which should be able to accommodate a certain level of entries and subsequently on the cost. Based on data collected from Member States, for the period 2010 - 2014, on average 700,000 convictions of TCN are recorded across all Member States per year. Where data was not submitted, estimates were calculated on the basis of Member State TCN population.
- Availability of high quality fingerprints **–** The ICT Cost Assessment of the technical scenarios for the implementation of ECRIS TCN system, with pseudonymised fingerprints included, assumes that all Member States have a well-established process of acquiring high quality fingerprints of convicted TCN. Further details on the current state of play of availability, quality and access to fingerprints are presented in section 5.
- Volume of processing operations and storage of AFIS for ECRIS TCN – According to AFIS vendors, the costs of an AFIS system vary depending on the volume of processing operations (i.e. the number of searches) and the size of the storage (i.e. the number of fingerprints stored in the AFIS). The volume of processing operations and storage capacity was used as an input by AFIS vendors to estimate the costs related to the setup and/or upgrade of an AFIS in the Member States. Subsequently, the cost estimates provided by vendors were used in this study for the calculation of all cost items related to the setup of a dedicated AFIS and upgrade of an existing national AFIS. For the establishment of a central AFIS, eu-LISA provided the cost estimates based on their experience with EURODAC also taking into account the foreseen volume of processing operations and size of storage. The estimated volume of processing operations and storage for an AFIS in the context of ECRIS TCN exchanges is detailed extensively in Annex 3.
- Costs for using the sTESTA network – Currently the exchange of criminal record data among Member States is performed through ECRIS using the sTESTA network. sTESTA 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. Given time constraints, the impact on the use of sTESTA network for ECRIS TCN exchanges has not been assessed in this study. The cost estimates are

based on the optimistic assumption that the existing sTESTA access point and bandwidth currently deployed in Member States and used in the context of ECRIS would be reused for the exchange of TCN fingerprints. 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 sTESTA network for the ECRIS TCN exchanges.

- Labour Daily Rates – costs collected in person day[50] were converted into costs (monetary figures) using the labour daily rates to convert person days into Euros. The labour rates are provided by Eurostat's structural earnings' survey of 2010 for occupation group ISCO 3 (Technicians and associate professionals). Figure 47 presents the labour daily rates per Member States in Euro.

Figure 47 Labour Daily Rates per MS in Euro[51]



Source: Eurostat's structural earnings survey, 2010.

- Data Sources and data extrapolation: The cost assessment is based on data collected through desk research activities, cost estimates provided by AFIS vendors and ECRIS technical specialists, as well as costs estimates provided by eu-LISA and FIU.net, as an input to the ICT assessment on ECRIS TCN conducted in 2015. Data extrapolation techniques were used whenever data was missing or data was considered inconsistent.

- Round of numbers: This study applies the general recommendations[52] 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, numbers are presented rounded to thousands or millions. Due to rounding, some totals may not correspond with the sum of the separate figures.

[50] This includes costs collected in fraction of a day, hours and minutes.
[51] Eurostat's structural earnings survey for occupation group ISCO 3 (Technicians and associate professionals), 2010.
[52] Eurostat tutorial on rounding of numbers available at: http://ec.europa.eu/eurostat/statistics-explained/index.php/Tutorial:Rounding_of_numbers

7.2.2 Cost assessment of Scenarios 1A & 1B

This section provides a qualitative description, assumptions and quantitative cost estimations related to the cost items comprising Scenarios 1A and 1B. This information is presented as follows:

- Table 6 presents a tabular view of qualitative descriptions, assumptions and quantitative cost estimates per cost item and per stakeholder group (European Union and Member States) related to Scenario 1A;
- Table 7 presents a summary of the quantitative cost estimates related to Scenario 1A detailing the break-down into type of costs (one-off and recurring).
- Table 8 presents a tabular view of qualitative descriptions, assumptions and quantitative cost estimates per cost item and per stakeholder group (European Union and Member States) related to Scenario 1B;
- Table 9 presents a summary of the quantitative cost estimates related to Scenario 1B detailing the break-down into type of costs (one-off and recurring);
- Figure 48 and Figure 49 present a graphical view of the quantitative cost estimates (one-off and recurring) per stakeholder group (European Union and Member States) for both Scenarios 1A and 1B.

Table 6 Scenario 1A: Cost elements

Stakeholder group	Scenario 1A Cost element	One-off	Recurring (Yearly)	Total Costs
Costs for the European Union	**Technical specification for an ECRIS TCN system** • **Description:** This cost item consists of the development of the technical specifications (documentation) for an ECRIS TCN system. The technical specifications aim at guiding the overall implementation of the ECRIS TCN system in Member States. The cost related to the technical specifications varies according to the number and complexity of the technical interfaces that need to be specified. For this scenario the specifications would include: ○ Specification of the technical interfaces for integration of the ECRIS TCN system at national level with ECRIS and CRR, as well as integration with national AFIS for providing input and performing local searches; ○ Specification of the technical interface for automated dissemination of FP files with other Member States. • **Assumptions:** Maintenance of the technical specifications is assumed to be included in the overall maintenance of the ECRIS project.	197		197
	Update of the ECRIS technical specifications • **Description**: This cost item consists of the update the technical specification (documentation) of ECRIS in order to accommodate the changes added due to the new ECRIS TCN system components and ECRIS TCN principles (one-to-many communication). These technical specifications are documents that enable Member States to implement their own implementation of ECRIS. • **Assumptions:** Maintenance of the technical specifications is assumed to be included in the overall maintenance of the ECRIS project.	88		88
	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 ECRIS TCN system components and ECRIS TCN principles (one-to-many communication). • **Assumptions:** Maintenance of the ECRIS RI is assumed to be included in the overall maintenance of the ECRIS project.	259		259
	Development of the ECRIS TCN system Reference Implementation • **Description:** This cost item consists of the development of the software component for ECRIS TCN system. The cost related to the development of the ECRIS TCN Reference Implementation varies according to the number and complexity of the software components to be developed. This scenario would include: ○ Technical interfaces for integration at national level with the CRR and with ECRIS; ○ Technical interface for automated dissemination and synchronisation of the exchange of FP files with Member States; ○ Integrated matching mechanism for performing queries on TCN using FP (integration with national AFIS) and alphanumeric data. • **Assumptions**: The following is assumed: ○ Licences and hardware costs are accounted under cost item 'Set-up of ECRIS TCN system'. ○ Member States implement the Reference Implementation. ○ Additional cost incurred by Member States opting for an alternative national implementation other than the Reference Implementation is not a cost mandated by the legislation and is therefore out of scope of this assessment.	986	197	1,183
	Training on the use of fingerprints functionalities of ECRIS TCN system • **Description:** Training of officials using ECRIS to search using fingerprints. • **Assumptions:** Training 2 trainers of each National Competent Authority.		111	111
	Total costs: European Union ***(in thousand EUR)***	**1,530**	**308**	**1,838**

Stakeholder group	Scenario 1A Cost element	One-off	Recurring (Yearly)	Total Costs
Costs for Member States	**Setup of a dedicated AFIS system to support the ECRIS TCN system** • **Description:** This cost item consists of an AFIS system capable of: ○ Pseudonymised FP file given as input by the national CA; ○ Automatically distribute FP files (new, changes and deletions) to the other ECRIS TCN systems across Member States; ○ Receive FP files from the other ECRIS TCN systems; ○ Store the FP file with a unique national identifier (database); ○ Answer fully automatically to local "hit/no hit" queries on TCN. • **Assumptions:** The estimated costs are based on the assumption that the AFIS system would be able to cope with the volume of searches and storage expected in the ECRIS TCN system as detailed in Annex 3. For scenario 1A, a storage volume of 2.1 Tb over 5 years is expected, as each Member State stores the fingerprints of all TCNs convicted in all Member States (high storage volume compared with scenario 2). However, as searches are performed locally in the dedicated AFIS, the number of searches are expected to be proportional to the number of convicted TCN in each Member State (e.g. countries with high number of convictions would need higher processing capacity and vice versa).	38,081	8,614	46,695
	Set up the ECRIS TCN system for local query in the dedicated AFIS • **Description:** This cost item consists of implementing and configuring the ECRIS TCN system Reference Implementation at national level. This includes: ○ Installing the ECRIS TCN system Reference Implementation in the Member States Premises: installing and testing the integration between the dedicated AFIS, ECRIS RI, Alphanumeric component (Ma3tch). ○ Installing, testing and calibrating the AFIS System; ○ Connecting the ECRIS TCN system with the CRR and ECRIS; ○ Establishing and testing the connection with the ECRIS TCN system of the other 27 Member States. • **Assumptions:** The following is assumed: ○ The integration of ECRIS TCN system in the national workflow for uploading FP into the ECRIS TCN system is excluded from the cost assessment. ○ No incremental cost on the network is incurred given that ECRIS is already using sTESTA. ○ It is assumed that the Reference Implementation can reuse hardware and server licenses from the ECRIS project, therefore no incremental cost for software and hardware is accounted.	7,000	1,960	8,960
	Total costs: Member States ***(in thousand EUR)***	45,081	10,574	55,655
	Total costs: European Union and Member States ***(in thousand EUR)***	**46,611**	**10,882**	**57,493**

Source: KURT SALMON Data Analysis, April 2016.

According to the ICT Cost Assessment, the total cost to implement Scenario 1A is EUR 57.4 million including one-off costs (i.e. initial investment) and recurring costs (i.e. one year operating costs). It should be noted that approximately 81% (EUR 46.5 million) of the total costs of Scenario 1A relates to the setting up of a dedicated AFIS system to support the ECRIS TCN system, which is incurred by Member States. The costs associated with the setup of a dedicated AFIS are, in scenario 1A, mostly related to the one-off costs (i.e. software, hardware and development costs). Specifically, if compared to the costs of setting up a dedicated AFIS in scenario 2A, costs related to the software (licenses) are significantly higher in scenario 1A (EUR 13.1 million) than in scenario 2A (EUR 6.6 million)[53]. Also, the one-off cost and the recurring costs are higher for the 28 Member States compared to what is incurred by the European Union. Table 7 presents a consolidated

[53] The estimated costs related to each cost item is further detailed into cost types (i.e. software, hardware, development, maintenance, support and training) in.

view on the one-off and recurring yearly costs incurred by the European Union and the 28 Member States for the implementation of Scenario 1A.

Table 7 Scenario 1A: Total costs summary (Fingerprints)

Estimated costs (*in thousand EUR*)	One-off costs	Recurring costs (Yearly)
Scenario 1A		
European Union	1,530	308
Member States	45,081	10,574
Total	**46,611**	**10,882**

Source: KURT SALMON Data Analysis, April 2016.

Both Scenarios 1A and 1B foresee the dissemination of pseudonymised TCN fingerprints to all other Member States for storage in their national ECRIS TCN systems. In Scenario 1A Member States rely on a dedicated AFIS while Scenario 1B is based on the reuse of an existing National AFIS. Table 8 presents in detail the cost elements composing Scenario 1B.

Table 8 Scenario 1B: Cost elements

Stakeholder group	Scenario 1B Cost element	One-off	Recurring (Yearly)	Total Costs
Costs for the European Union	**Technical specification for an ECRIS TCN system** • **Description:** This cost item consists of the development of the technical specifications (documentation) for an ECRIS TCN system. The technical specifications aim at guiding the overall implementation of the ECRIS TCN system in Member States. The cost related to the technical specifications varies according to the number and complexity of the technical interfaces that need to be specified. For this scenario the specifications would include: ○ Specification of the technical interfaces for integration of the ECRIS TCN system at national level with ECRIS and CRR, as well as integration with national AFIS for performing local searches. ○ Specification of the technical interface for automated dissemination of FP files with other Member States. • **Assumptions:** Maintenance of the technical specifications is assumed to be included in the overall maintenance of the ECRIS project.	191		191
	Update of the ECRIS technical specifications • **Description**: This cost item consists of the update of the technical specification (documentation) of ECRIS in order to accommodate the changes added due to the new ECRIS TCN system components and ECRIS TCN principles (one-to-many communication). These technical specifications are documents that enable Member States to implement their own implementation of ECRIS. • **Assumptions:** Maintenance of the technical specifications is assumed to be included in the overall maintenance of the ECRIS project.	88		88
	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 ECRIS TCN system components and ECRIS TCN principles (one-to-many communication). • **Assumptions:** Maintenance of the ECRIS RI is assumed to be included in the overall maintenance of the ECRIS project.	259		259
	Development of the ECRIS TCN system Reference Implementation for local queries in a national AFIS • **Description:** This cost item consists of the development of the software component for ECRIS TCN system. The cost related to the development of the ECRIS TCN Reference Implementation varies according to the number and complexity of the software components to be developed. This scenario would include: ○ Technical interfaces for integration at national level with the CRR, ECRIS and national AFIS. ○ Technical interface for automated dissemination and synchronisation of FP files with Member States; ○ Integrated matching mechanism for performing queries on TCN using FP (integration with national AFIS) and alphanumeric data ○ Software application that interfaces the national AFIS in order to: ○ Pseudonymisation/protection of the FP files extracted from the national AFIS; ○ Automatically distributes pseudonymised/protected FP files (new, changes and deletions) to the other ECRIS TCN system across Member States; ○ Receives pseudonymised/protected FP files from the other ECRIS TCN system; ○ Stores the received FP files in the national AFIS; ○ Interfaces the national AFIS for performing "hit/no hit" queries (one-to-many matching) on TCN. • **Assumptions**: The following is assumed: ○ Member States implement the Reference Implementation. ○ Additional cost incurred by Member States opting for an alternative national implementation other than the Reference Implementation is not a cost mandated by the legislation and is therefore out of scope of this assessment.	974	195	1,169
	Training on the use of fingerprints functionalities of ECRIS TCN system • **Description:** Training of officials using ECRIS to search using fingerprints. • **Assumptions:** Training 2 trainers of each National Competent Authority.		111	111
	Total costs: European Union ***(in thousand EUR)***	**1,512**	**306**	**1,818**

Stakeholder group	Scenario 1B Cost element	One-off	Recurring (Yearly)	Total Costs
Costs for Member States	**Set up the ECRIS TCN system for local query in the national AFIS** • **Description:** This cost item consists of implementing and configuring the ECRIS TCN system Reference Implementation at national level. This includes: ○ Installing the ECRIS TCN system Reference Implementation in the Member States premises; this includes installing and testing the integration between the national AFIS, ECRIS RI, and the alphanumeric component (Ma3tch). ○ Connecting the ECRIS TCN system with the CRR and ECRIS; ○ Connecting the ECRIS TCN system with the National AFIS; ○ Establishing the connection with the ECRIS TCN system of the other 27 Member States. • **Assumptions:** The following is assumed: ○ The integration of ECRIS TCN system in the national workflow for uploading FP into the ECRIS TCN system is excluded from the cost assessment. ○ No incremental cost on the network is incurred given that ECRIS is already using sTESTA. ○ It is assumed that the Reference Implementation can reuse hardware and server licenses from the ECRIS project, therefore no incremental cost for software and hardware is accounted.	7,000	1,960	8,960
	Upgrade National AFIS • **Description:** This cost item consists of upgrading the national AFIS to accommodate the requirements of storing and matching TCN fingerprints as described in Annex 3. For scenario 1B an incremental storage volume of 2.1 Tb over 5 years is expected, taking into account that each Member State stores the fingerprints of all TCNs convicted in all Member States (high storage volume compared with scenario 2). However, as searches are performed locally in the national AFIS, the number of incremental searches is expected to be proportional to the number of convicted TCN in each Member State (e.g. countries with a high number of convictions would need higher processing capacity and vice versa). • **Assumptions:** The following is assumed: ○ No incremental maintenance and support due to the reuse of existing AFIS.	18,119		18,119
	Total costs: Member States ***(in thousand EUR)***	**25,119**	**1,960**	**27,079**
	Total costs: European Union and Member States ***(in thousand EUR)***	**26,632**	**2,266**	**28,897**

Source: KURT SALMON Data Analysis, April 2016.

According to the ICT Cost Assessment, the total cost to implement Scenario 1B is EUR 28.8 million including one-off costs (i.e. initial investment) and recurring costs (i.e. one year operating costs). Approximately 63% (EUR 18.1 million) of the total costs of Scenario 1B relates to the upgrading of the National AFIS, which is incurred by Member States. All the costs associated with the upgrading of the national AFIS are, in scenario 1B, related to the one-off costs (i.e. software licenses and development costs). Specifically, if compared to the costs of upgrading the national AFIS in scenario 2B, costs related to the software (licenses) are significantly higher in scenario 1B (EUR 7.8 million) than in scenario 2A (EUR 3.9 million)[54]. Also, the one-off cost and the recurring costs are higher for the 28 Member States compared to what is incurred by the European Union. Table 9 presents a consolidated view on the one-off and recurring costs incurred by the European Union and 28 Member States for the implementation of Scenario 1B.

[54] The estimated costs related to each cost item is further detailed into cost types (i.e. software, hardware, development, maintenance, support and training) in Annex 6.

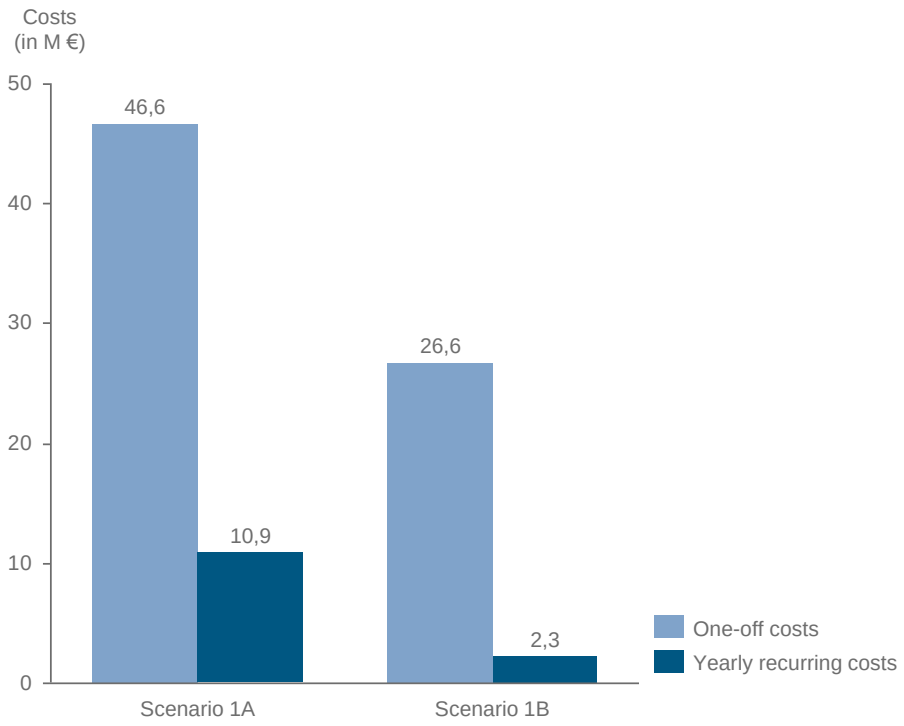
Table 9 Scenario 1B: Total costs summary (Fingerprints)

Estimated costs (*in thousand EUR*)	One-off costs	Recurring costs (Yearly)
Scenario 1B		
European Union	1,512	306
Member States	25,119	1,960
Total	**26,632**	**2,266**

Source: KURT SALMON Data Analysis, April 2016.

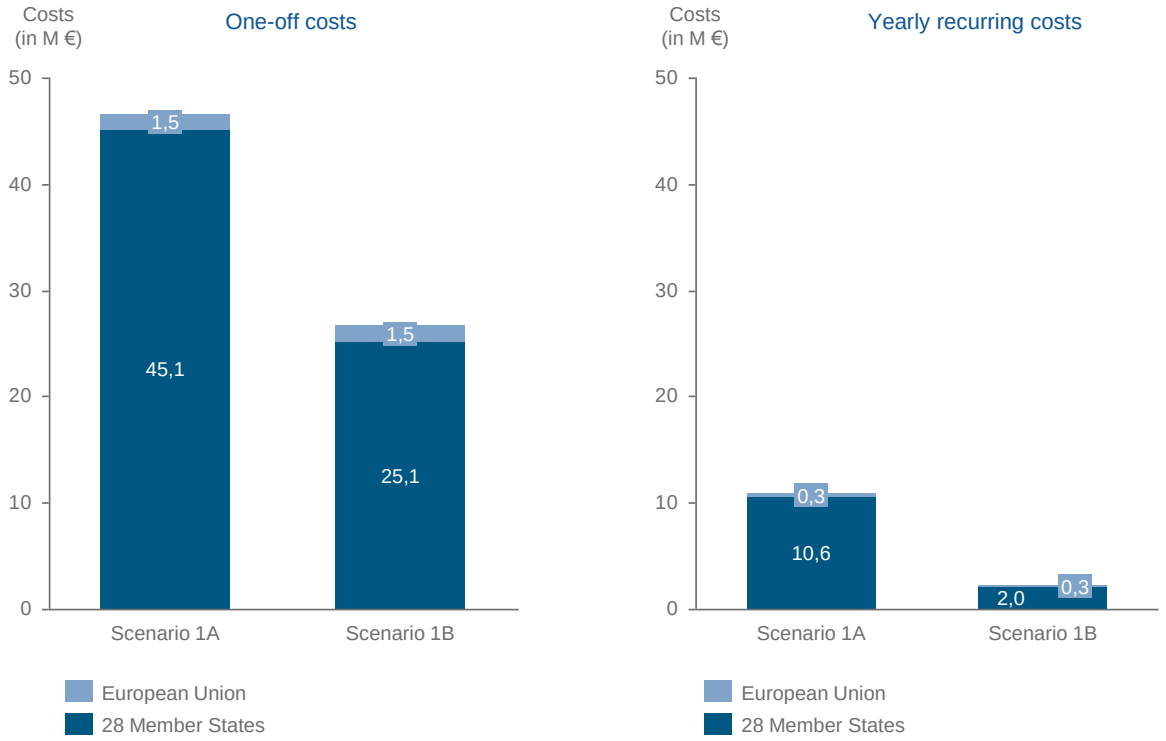
Finally, Figure 48 and Figure 49 present the comparison between Scenarios 1A and 1B in terms of total cost (one-off and recurring), as well as their distribution to the European Union and the 28 Member States stakeholder groups.

Figure 48 Scenario 1A & 1B: Total costs for Fingerprints (1/2)



As previously stated, the main difference between Scenario 1A and 1B (which significantly impacts the costs) is the reuse of an existing national AFIS in the case of Scenario 1B and the set-up of a dedicated AFIS to support the ECRIS TCN system in the case of Scenario 1A.

Figure 49 Scenario 1A & 1B: Total costs for Fingerprints (2/2)



7.2.3 Cost assessment of Scenarios 2A & 2B

This section provides a qualitative description, assumptions and quantitative cost estimations related to the cost items comprising Scenarios 2A and 2B. This information is presented as follows:

- Table 10 presents a tabular view of qualitative descriptions, assumptions and quantitative cost estimates per cost item and per stakeholder group (European Union and Member States) related to Scenario 2A;
- Table 11 presents a summary of the quantitative cost estimates related to Scenario 2A detailing the break-down into type of costs (one-off and recurring).
- Table 12 presents a tabular view of qualitative descriptions, assumptions and quantitative cost estimates per cost item and per stakeholder group (European Union and Member States) related to Scenario 2B;
- Table 13 presents a summary of the quantitative cost estimates related to Scenario 2B detailing the break-down into type of costs (one-off and recurring);
- Figure 50 and Figure 51 present a graphical view of the quantitative cost estimates (one-off and recurring) per stakeholder group (European Union and Member States) for both Scenarios 2A and 2B.

Table 10 Scenario 2A: Cost elements

Stakeholder group	Scenario 2A Cost element	One-off	Recurring (Yearly)	Total Costs
Costs for the European Union	**Technical specification for an ECRIS TCN system** • **Description:** This cost item consists of the development of the technical specifications (documentation) for an ECRIS TCN system. The technical specifications aim at guiding the overall implementation of the ECRIS TCN system in Member States. The cost related to the technical specifications varies according to the number and complexity of the technical interfaces that need to be specified. For this scenario the specifications would include: ○ Specification of the technical interfaces for integration of the ECRIS TCN system at national level with ECRIS and CRR; ○ Specifications for the integration with national AFIS for providing input, distributed search and aggregation of results. • **Assumptions:** Maintenance of the technical specifications is assumed to be included in the overall maintenance of the ECRIS project.	188		188
	Update of the ECRIS technical specifications • **Description**: This cost item consists of the update the technical specification (documentation) of ECRIS in order to accommodate the changes added due to the new ECRIS TCN system components and ECRIS TCN principles (one-to-many communication). These technical specifications are documents that enable Member States to implement their own implementation of ECRIS. • **Assumptions:** Maintenance of the technical specifications is assumed to be included in the overall maintenance of the ECRIS project.	88		88
	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 ECRIS TCN system components and ECRIS TCN principles (one-to-many communication). • **Assumptions:** Maintenance of the ECRIS RI is assumed to be included in the overall maintenance of the ECRIS project.	259		259
	Development of the ECRIS TCN system Reference Implementation • **Description:** This cost item consists of the development of the software component for ECRIS TCN system. The cost related to the development of the ECRIS TCN Reference Implementation varies according to the number and complexity of the software components to be developed. This scenario would include: ○ Technical interfaces for integration of the ECRIS TCN system at national level with the CRR and with ECRIS; ○ Technical interface for automated distributed "hit/no hit" search queries with Member States; ○ Integrated matching mechanism for performing queries on TCN using FP (integration with national AFIS) and alphanumeric data. • **Assumptions**: The following is assumed: ○ Licences and hardware is accounted under cost item ECRIS TCN FP store. ○ Member States implements the Reference Implementation. ○ Additional cost incurred by Member States opting for an alternative national implementation other than the Reference Implementation is not a cost mandated by the legislation and is therefore out of scope of this assessment.	970	194	1,164
	Training on the use of fingerprints functionalities of ECRIS TCN system • **Description:** Training of officials using ECRIS to search using fingerprints. • **Assumptions:** Training 2 trainers of each National Competent Authority.		111	111
	Total costs: European Union ***(in thousand EUR)***	**1,505**	**305**	**1,810**

Stakeholder group	Scenario 2A Cost element	One-off	Recurring (Yearly)	Total Costs
Costs for Member States	**Setup of a dedicated AFIS system to support the ECRIS TCN system** • **Description:** This cost item consists of an AFIS system able to: ○ Store FP files received from the national CA; ○ Perform "hit/no hit" queries (one-to-many matching) in the local FB database; ○ Trigger distributed "hit/no hit" queries (one-to-many matching) to the 27 other Member States; ○ Pseudonymise (keep only the tenprints images discarding other identification data) the FP files to be included in the distributed "hit/no hit" queries (one-to-many matching); ○ Collect, consolidate and present the results of the "hit/no hit" query responses (including handling of errors). • **Assumptions:** The estimated costs are based on the assumption that the AFIS system would be able to cope with the volume of searches and storage expected in the ECRIS TCN system as detailed in Annex 3. For Scenario 2A it is expected that each Member State stores only the fingerprints of TCNs convicted in their territory (lower storage volume compared with Scenario 1). However, as searches are distributed to all other Member States, the number of searches are not expected to be proportional to the number of convicted TCN in each Member State (e.g. countries with a low number of convictions would need higher processing capacity to respond to the searches originated by Member States with a high number of conviction and vice versa).	27,977	7,142	35,119
	Set up the ECRIS TCN system for distributed "hit/no hit" search queries in dedicated AFIS • **Description:** This cost item consists of implementing and configuring the ECRIS TCN system Reference Implementation at national level. This includes: ○ Installing the ECRIS TCN system Reference Implementation in the Member States premises: installing and testing the integration between the dedicated AFIS, ECRIS RI, Alphanumeric component (Ma3tch). ○ Installing, testing and calibrating the AFIS System; ○ Connecting the ECRIS TCN system with the CRR and ECRIS; ○ Establishing the connection with the ECRIS TCN system of the other 27 Member States. • **Assumptions:** The following is assumed: ○ The integration of ECRIS TCN system in the national workflow for uploading FP into the ECRIS TCN system is excluded from the cost assessment. ○ No incremental cost on the network is incurred given that ECRIS is already using sTESTA. ○ It is assumed that the Reference Implementation can reuse hardware and server licenses from the ECRIS project, therefore no incremental cost for software and hardware is accounted.	7,000	1,960	8,960
	Total costs: Member States ***(in thousand EUR)***	**34,977**	**9,102**	**44,079**
	Total costs: European Union and Member States ***(in thousand EUR)***	**36,482**	**9,407**	**45,889**

Source: KURT SALMON Data Analysis, April 2016.

According to the ICT Cost Assessment, the total cost to implement Scenario 2A is EUR 45.8 million including one-off costs (i.e. initial investment) and recurring costs (i.e. one year operating costs). Approximately 77% (EUR 35.1 million) of the total costs of scenario 2A relates to setting up a dedicated AFIS system to support the ECRIS TCN system, which is incurred by Member States. The costs associated to the setup of a dedicated AFIS, in scenario 2A, are mostly related to the one-off costs (i.e. software, hardware and development costs). As explained in section 7.2.2, if compared to the costs of setting up a dedicated AFIS in scenario 1A, costs related to the software (licenses) are significantly lower in scenario 2A (EUR 6.6 million)

than in scenario 1A (EUR 13.1 million)[55]. Also, the one-off cost and the recurring costs are higher for the 28 Member States compared to what is incurred by the European Union. Table 11 presents a consolidated view on the one-off and recurring costs incurred by the European Union and the 28 Member States for the implementation of Scenario 2A.

Table 11 Scenario 2A: Total costs summary (Fingerprints)

Estimated costs (*in thousand EUR*)	One-off costs	Recurring costs (Yearly)
Scenario 2A		
European Union	1,512	305
Member States	34,977	9,102
Total	**36,482**	**9,407**

Source: KURT SALMON Data Analysis, April 2016.

The main difference between Scenarios 2 and Scenarios 1, is the dissemination of TCN fingerprints. Scenarios 1 disseminate TCN fingerprints to all Member States while in Scenarios 2 the fingerprints are not disseminated but the "hit/no hit" searches with fingerprints are performed over all Member States. On the other hand, similarly to Scenarios 1A and 1B, Scenario 2A foresees the set-up of a dedicated AFIS while Scenario 2B reuses an existing National AFIS. Table 8 provides in detail the cost elements composing Scenario 2B.

[55] The estimated costs related to each cost item is further detailed into cost types (i.e. software, hardware, development, maintenance, support and training) in Annex 6.

Table 12 Scenario 2B: Cost elements

Stakeholder group	Scenario 2B Cost element	One-off	Recurring (Yearly)	Total Costs
Costs for the European Union	**Technical specification for an ECRIS TCN system** • **Description:** This cost item consists of the development of the technical specifications (documentation) for an ECRIS TCN system. The technical specifications aim at guiding the overall implementation of the ECRIS TCN system in Member States. These specifications would include: ○ Specification of the technical interfaces for integration of the ECRIS TCN system at national level with ECRIS and CRR. ○ Specifications for the integration with national AFIS for distributed search and aggregation of results. • **Assumptions:** Maintenance of the technical specifications is assumed to be included in the overall maintenance of the ECRIS project.	180		180
	Update of the ECRIS technical specifications • **Description**: This cost item consists of the update the technical specification (documentation) of ECRIS in order to accommodate the changes added due to the new ECRIS TCN system components and ECRIS TCN principles (one-to-many communication). These technical specifications are documents that enable Member States to implement their own implementation of ECRIS. • **Assumptions:** Maintenance of the technical specifications is assumed to be included in the overall maintenance of the ECRIS project.	88		88
	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 ECRIS TCN system components and ECRIS TCN principles (one-to-many communication). • **Assumptions:** Maintenance of the ECRIS RI is assumed to be included in the overall maintenance of the ECRIS project.	259		259
	Development of the ECRIS TCN system Reference Implementation for distributed queries • **Description:** This cost item consists of the development of the software component for ECRIS TCN system. The cost related to the development of the ECRIS TCN Reference Implementation varies according to the number and complexity of the software components to be developed. This scenario would include: : ○ Technical interfaces for integration of the ECRIS TCN system at national level with the CRR and with ECRIS; ○ Technical interface for automated distributed "hit/no hit" search queries with Member States; ○ Integrated matching mechanism for performing queries on TCN using FP (integration with national AFIS) and alphanumeric data; ○ A software application that interfaces the national AFIS in order to: ○ Pseudonymise/protect (keep only the tenprints images discarding other identification data) the FP files extracted from the national AFIS and included them in the distributed "hit/no hit" queries (one-to-many matching); ○ Trigger distributed "hit/no hit" queries (one-to-many matching) to the 27 other Member States; ○ Collect, consolidate and present the results of the hit/no hit query responses (including handling of errors); ○ Interfaces the national AFIS for performing "hit/no hit" queries (one-to-many matching) on TCN. • **Assumptions**: The following is assumed: ○ Licences and hardware is accounted under cost item ECRIS TCN FP store. ○ Member States implements the Reference Implementation. ○ Additional cost incurred by Member States opting for an alternative national implementation other than the Reference Implementation is not a cost mandated by the legislation and is therefore out of scope of this assessment.	957	191	1,148
	Training on the use of fingerprints functionalities of ECRIS TCN system • **Description:** Training of officials using ECRIS to search using fingerprints. • **Assumptions:** Training 2 trainers of each National Competent Authority.		111	111
	Total costs: European Union ***(in thousand EUR)***	**1,484**	**302**	**1,786**

Stakeholder group	Scenario 2B Cost element	One-off	Recurring (Yearly)	Total Costs
Costs for Member States	**Set up the ECRIS TCN system for distributed "hit/no hit" search queries in national AFIS** • **Description:** This cost item consists of implementing and configuring the ECRIS TCN system Reference Implementation at national level. This includes: ○ Installing the ECRIS TCN system Reference Implementation in the Member States premises; this includes installing and testing the integration between the national AFIS, ECRIS RI, and the alphanumeric component (Ma3tch) ○ Connecting the ECRIS TCN system with the CRR and ECRIS ○ Connecting the ECRIS TCN system with the National AFIS; ○ Establishing the connection with the ECRIS TCN system of the other 27 Member States • **Assumptions:** The following is assumed: ○ The integration of ECRIS TCN system in the national workflow for uploading FP into the ECRIS TCN system is excluded from the cost assessment. ○ No incremental cost on the network is incurred given that ECRIS is already using sTESTA. ○ It is assumed that the Reference Implementation can reuse hardware and server licenses from the ECRIS project, therefore no incremental cost for software and hardware is accounted	7,000	1,960	8,960
	Upgrade of National AFIS • **Description:** This cost item consists of upgrading the national AFIS with additional storage and processing capacity to handle fingerprints for ECRIS TCN purpose as detailed in Annex 3. For Scenario 2B it is expected that each Member State stores only the fingerprints of TCNs convicted in their territory (lower storage volume compared with Scenario 1). However, as searches are distributed to all other Member States, the number of incremental searches to be handle by the national AFIS is not expected to be proportional to the number of convicted TCN in each Member State (e.g. countries with a low number of convictions would need higher processing capacity to respond to the searches originated by Member States with a high number of conviction and vice versa). • **Assumptions:** The following is assumed: ○ No incremental maintenance and support due to the reuse of existing AFIS.	13,482		13,482
	Total costs: Member States ***(in thousand EUR)***	20,482	1,960	22,442
	Total costs: European Union and Member States ***(in thousand EUR)***	**21,966**	**2,262**	**24,228**

Source: KURT SALMON Data Analysis, April 2016.

According to the ICT Cost Assessment, the total cost to implement Scenario 2B is approximately EUR 24.2 million including one-off costs (i.e. initial investment) and recurring costs (i.e. one year operating costs). Approximately 56% (EUR 13.5 million) of the total costs of Scenario 2B relates to the upgrade the National AFIS, which is incurred by Member States. All the costs associated to the upgrading of the national AFIS, in scenario 2B, are related to the one-off costs (i.e. software licenses and development costs). As explained in section 7.2.2, if compared to the costs of upgrading the national AFIS in scenario 1B, costs related to the software (licenses) are significantly lower in scenario 2B (EUR 3.9 million) than in scenario 1B (EUR 7.8 million)[56]. Also, the one-off cost and the recurring costs are higher for the 28 Member States compared to what is incurred by the European Union. Table 13 presents a consolidated view on the one-off and recurring costs incurred by the European Union and 28 Member States for the implementation of Scenario 2B.

[56] The estimated costs related to each cost item is further detailed into cost types (i.e. software, hardware, development, maintenance, support and training) in Annex 6.

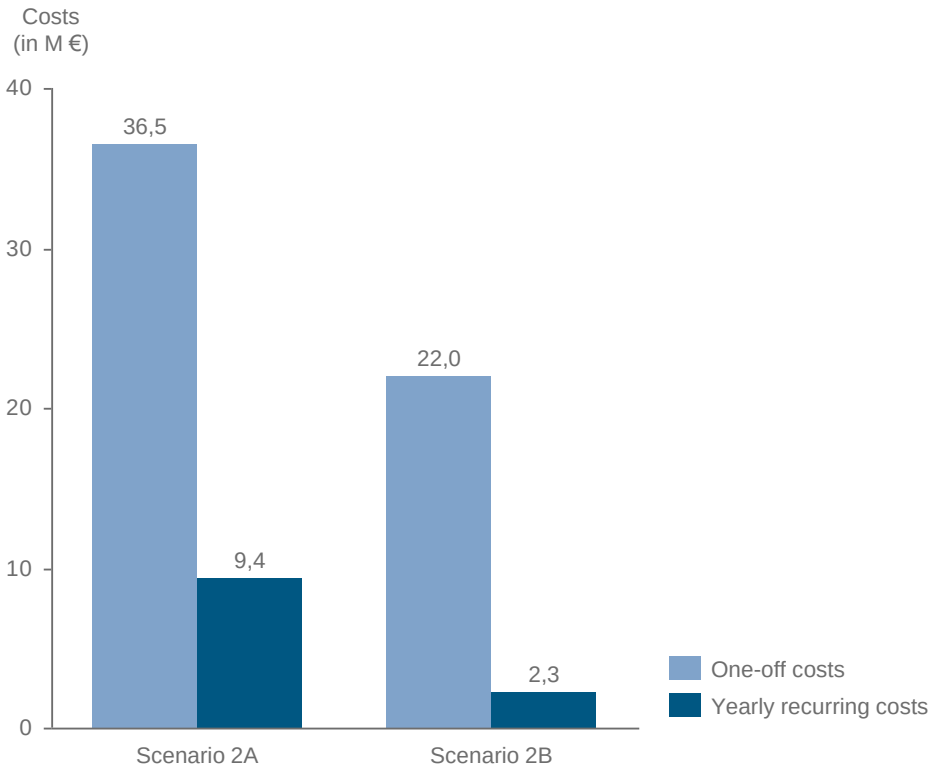
Table 13 Scenario 2B: Total costs summary (Fingerprints)

Estimated costs (*in thousand EUR*)	One-off costs	Recurring costs (Yearly)
Scenario 2B		
European Union	1,484	302
Member States	20,482	1,960
Total	**21,966**	**2,262**

Source: KURT SALMON Data Analysis, April 2016.

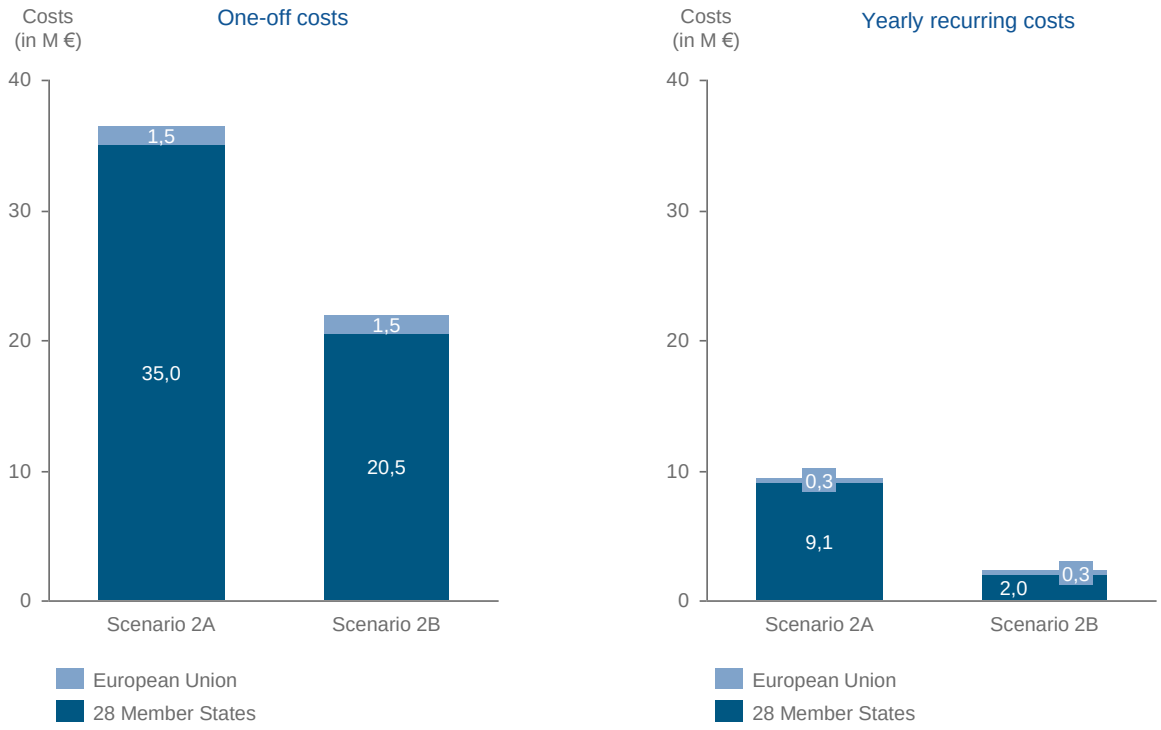
Finally, Figure 50 and Figure 51 present the comparison between Scenarios 2A and 2B in terms of total cost (one-off and recurring) as well as their distribution to the European Union and the 28 Member States.

Figure 50 Scenario 2A & 2B: Total costs for Fingerprints (1/2)



Similar to Scenarios 1A and 1B, the main difference between Scenarios 2A and 2B (which significantly impacts the costs) is the reuse of an existing national AFIS in the case of Scenario 2B and the setting-up of a dedicated AFIS to support the ECRIS TCN system in the case of Scenario 2A.

Figure 51 Scenario 2A & 2B: Total costs for Fingerprints (2/2)



7.2.4 Cost assessment of Scenarios 3A & 3B

This section provides a qualitative description, assumptions and quantitative cost estimations related to the cost items comprising Scenario 3A and 3B. This information is presented as follows:

- Table 14 presents a tabular view of qualitative descriptions, assumptions and quantitative cost estimates per cost item and per stakeholder group (European Union and Member States) related to Scenario 3A;
- Table 15 presents a summary of the quantitative cost estimates related to Scenario 3A detailing the break-down into type of costs (one-off and recurring);

Table 16 presents a tabular view of qualitative descriptions, assumptions and quantitative cost estimates per cost item and per stakeholder group (European Union and Member States) related to Scenario 3B;

- Table 17 presents a summary of the quantitative cost estimates related to Scenario 3B detailing the break-down into type of costs (one-off and recurring);
- Figure 52 and Figure 53 present a graphical view of the quantitative cost estimates (one-off and recurring) per stakeholder group (European Union and Member States) for both Scenarios 3A and 3B.

Table 14 Scenario 3A: Cost elements

Stakeholder group	Scenario 3A Cost element	One-off	Recurring (Yearly)	Total Costs
Costs for the European Union	**Technical specification for an ECRIS TCN system** • **Description:** This cost item consists of the development of the technical specifications (documentation) for an ECRIS TCN system. The technical specifications aim at guiding the overall implementation of the ECRIS TCN system in Member States. The cost related to the technical specifications varies according to the number and complexity of the technical interfaces that need to be specified. For this scenario the specifications would include: ○ Specification of the technical interfaces for integration of the ECRIS TCN system at national level with ECRIS and CRR; ○ Specifications for integration with central AFIS for providing input, searches and central storage of FP files; ○ Specification of the technical interface for automated distributed "hit/no hit" search queries with other Member States (for alphanumeric data). • **Assumptions:** Maintenance of the technical specifications is assumed to be included in the overall maintenance of the ECRIS project.	186		186
	Update of the ECRIS technical specifications • **Description**: This cost item consists of the update the technical specification (documentation) of ECRIS in order to accommodate the changes added due to the new ECRIS TCN system components. These technical specifications are documents that enable Member States to implement their own implementation of ECRIS. • **Assumptions:** Maintenance of the technical specifications is assumed to be included in the overall maintenance of the ECRIS project.	88		88
	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 ECRIS TCN system components and ECRIS TCN principles (one-to-many communication). • **Assumptions:** Maintenance of the ECRIS RI is assumed to be included in the overall maintenance of the ECRIS project.	259		259
	Development of the ECRIS TCN system Reference Implementation • **Description:** This cost item consists of the development of the software component for ECRIS TCN system. The cost related to the development of the ECRIS TCN Reference Implementation varies according to the number and complexity of the software components to be developed. This scenario would include: ○ Technical interfaces for integration of the ECRIS TCN system at national level with the CRR and with ECRIS. ○ Technical interface for automated distributed "hit/no hit" search queries with Member States (alphanumeric data). ○ Technical interface with the central AFIS. ○ Integrated matching mechanism for performing queries on TCN using FP (integration with central AFIS) and alphanumeric data. ○ Application for sending updates on inclusion/removal of FP file to the central AFIS. ○ TCN fingerprint storage. • **Assumptions**: The following is assumed: ○ Member States implement the Reference Implementation. ○ Additional costs incurred by Member States opting for an alternative national implementation are not costs mandated by the legislation and are therefore out of scope of this assessment.	931	186	1,117
	Set up of central AFIS system • **Description:** This cost item consists of the implementation of a centralised AFIS system at EU level managed by a European Institution or Agency (e.g. eu-LISA). • **Assumptions:** The estimated costs are based on the assumption that the central AFIS system would be able to cope with up to 3.5 thousand searches per day and 2.1 Tb of storage as expected in the ECRIS TCN system and detailed in Annex 3.	1,950	458	2,408
	Training on the use of fingerprints functionalities of ECRIS TCN system • **Description:** Training of officials using ECRIS to search using fingerprints. **Assumptions:** Training 2 trainers of each National Competent Authority.		111	111
	Total costs: European Union (in thousand EUR)	**3,414**	**755**	**4,170**

Stakeholder group	Scenario 3A Cost element	One-off	Recurring (Yearly)	Total Costs
Costs for Member States	**Set up the ECRIS TCN system at national level for querying a Central AFIS** • **Description:** 'This cost item consists of implementing and configuring the ECRIS TCN system Reference Implementation at national level. This includes: ○ Installing the ECRIS TCN system Reference Implementation in the Member States Premises; this includes installing and testing the integration between the central AFIS, ECRIS RI, Alphanumeric component (Ma3tch). ○ Connecting the ECRIS TCN system with the CRR and ECRIS. ○ Connecting the ECRIS TCN system with the central AFIS. • **Assumptions:** The following is assumed: ○ The integration of ECRIS TCN system in the national workflow for uploading FP into the ECRIS TCN system is excluded from the cost assessment. ○ No incremental cost on the network is incurred given that ECRIS is already using sTESTA. ○ It is assumed that the Reference Implementation can reuse hardware and server licenses from the ECRIS project, therefore no incremental cost for software and hardware is accounted.	3,500	1,260	4,760
	Total costs: Member States (in thousand EUR)	**3,500**	**1,260**	**4,760**
	Total costs: European Union and Member States *(in thousand EUR)*	**6,914**	**2,015**	**8,930**

Source: KURT SALMON Data Analysis, April 2016.

According to the ICT Cost Assessment, the total cost to implement Scenario 3A is EUR 8.9 million including one-off costs (i.e. initial investment) and recurring costs (i.e. one year operating costs). Approximately 53% (EUR 4.7 million) of the total costs of Scenario 3A relates to the setting up the ECRIS TCN system at national level by the 28 Member States for querying a central AFIS. The costs associated with the setting up the ECRIS TCN system, in scenario 3A, are mostly related to the development costs for implementing and configuring the ECRIS TCN system (EUR 3.5 million)[57]. The one-off cost and the recurring costs are slightly higher for the 28 Member States compared to what is incurred by the European Union. Table 15 presents a consolidated view on the one-off and recurring costs incurred by the European Union and the 28 Member States for the implementation of Scenario 3A.

Table 15 Scenario 3A: Total costs summary (Fingerprints)

Estimated costs (*in thousand EUR*)	One-off costs	Recurring costs (Yearly)
Scenario 3A		
European Union	3,414	755
Member States	3,500	1,260
Total	**6,914**	**2,015**

Source: KURT SALMON Data Analysis, April 2016.

Both Scenarios 3A and 3B are based on a central AFIS managed by eu-LISA with an automated "hit/no hit" search with TCN FP. The difference between Scenarios 3A and 3B is that in Scenario 3A the verification of FP is performed without the support of an AFIS at national level, and in Scenario 3B the verification of FP is performed with support of an AFIS. Table 16 presents in details the cost elements composing Scenario 3B.

[57] The estimated costs related to each cost item is further detailed into cost types (i.e. software, hardware, development, maintenance, support and training) in Annex 6.

Table 16 Scenario 3B: Cost elements

Stakeholder group	Scenario 3B Cost element	One-off	Recurring (Yearly)	Total Costs
Costs for the European Union	**Technical specification for an ECRIS TCN system** • **Description:** This cost item consists of the development of the technical specifications (documentation) for an ECRIS TCN system. The technical specifications aim at guiding the overall implementation of the ECRIS TCN system in Member States. The cost related to the technical specifications varies according to the number and complexity of the technical interfaces that need to be specified. For this scenario the specifications would include: ○ Specification of the technical interfaces for integration of the ECRIS TCN system at national level with ECRIS and CRR; ○ Specifications for integration with central AFIS for providing input, searches and central storage of FP files; ○ Specification of the technical interface for automated distributed "hit/no hit" search queries with other Member States (for alphanumeric data). • **Assumptions:** Maintenance of the technical specifications is assumed to be included in the overall maintenance of the ECRIS project.	186		186
	Update of the ECRIS technical specifications • **Description**: This cost item consists of the update of the technical specification (documentation) of ECRIS in order to accommodate the changes added due to the new ECRIS TCN system components. These technical specifications are documents that enable Member States to implement their own implementation of ECRIS. • **Assumptions:** Maintenance of the technical specifications is assumed to be included in the overall maintenance of the ECRIS project.	88		88
	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 ECRIS TCN system components and ECRIS TCN principles (one-to-many communication). • **Assumptions:** Maintenance of the ECRIS RI is assumed to be included in the overall maintenance of the ECRIS project.	259		259
	Development of the ECRIS TCN system Reference Implementation • **Description:** This cost item consists of the development of the software component for ECRIS TCN system. The cost related to the development of the ECRIS TCN Reference Implementation varies according to the number and complexity of the software components to be developed. This scenario would include: ○ Technical interfaces for integration of the ECRIS TCN system at national level with the CRR and with ECRIS. ○ Technical interface for automated distributed "hit/no hit" search queries with Member States (alphanumeric data). ○ Technical interface with the central AFIS. ○ Integrated matching mechanism for performing queries on TCN using FP (integration with central AFIS) and alphanumeric data. ○ Application for sending updates on inclusion/removal of FP file to the central AFIS. • **Assumptions**: The following is assumed: ○ Member States will be able to use the Reference Implementation. ○ Additional cost on opting for a national implementation is not a cost mandated by the legislation.	931	186	1,117
	Set up of central AFIS system • **Description:** This cost item consists of the complete implementation of a centralised AFIS system at EU level managed by a European Institution or Agency (e.g. eu-LISA). • **Assumptions:** The estimated costs are based on the assumption that the central AFIS system would be able to cope with up to 3.5 thousand searches per day and 2.1 Tb of storage as expected in the ECRIS TCN system and detailed in Annex 3.	1,950	458	2,408
	Training on the use of fingerprints functionalities of ECRIS TCN system • **Description:** Training of officials using ECRIS to search using fingerprints. **Assumptions:** Training 2 trainers of each National Competent Authority.		111	111
	Total costs: European Union (in thousand EUR)	**3,414**	**755**	**4,170**

Stakeholder group	Scenario 3B Cost element	One-off	Recurring (Yearly)	Total Costs
Costs for Member States	**Set up the ECRIS TCN system at national level for querying a central AFIS** • **Description:** 'This cost item consists of implementing and configuring the ECRIS TCN system Reference Implementation at national level. This includes: ○ Installing the ECRIS TCN system Reference Implementation in the Member States Premises; this includes installing and testing the integration between the central AFIS, ECRIS RI, Alphanumeric component (Ma3tch). ○ Connecting the ECRIS TCN system with the CRR and ECRIS. ○ Connecting the ECRIS TCN system with the central AFIS. • **Assumptions:** The following is assumed: ○ The integration of ECRIS TCN system in the national workflow for uploading FP into the ECRIS TCN system is excluded from the cost assessment. ○ No incremental cost on the network is incurred given that ECRIS is already using sTESTA. ○ It is assumed that the Reference Implementation can reuse hardware and server licenses from the ECRIS project, therefore no incremental cost for software and hardware is accounted.	3,500	1,260	4,760
	Upgrade National AFIS for verification following a query in the central AFIS • **Description:** AFIS. In case of a "hit", upon a request of a Member State, the requested Member State might decide to perform a verification based on fingerprints transmitted with the request. In this scenario it is assumed that the requested Member States will use the national AFIS to perform the verification process. Therefore this cost item includes the incremental development and software costs for upgrading the national AFIS to accommodate the requirements of verifying TCN fingerprints following a "hit/no hit" search query at the central • **Assumptions:** The following is assumed: ○ No incremental hardware, maintenance and support due to the reuse of existing AFIS.	8,988		8,988
	Total costs: Member States (in thousand EUR)	12,488	1,260	13,748
	Total costs: European Union and Member States *(in thousand EUR)*	**15,902**	**2,015**	**17,917**

Source: KURT SALMON Data Analysis, April 2016.

According to the ICT Cost Assessment, the total cost to implement Scenario 3B is EUR 17.9 million including one-off costs (i.e. initial investment) and recurring costs (i.e. one year operating costs). Approximately 50% of the total costs relates to the upgrading the National AFIS for verification following a query in the central AFIS, which is incurred by Member States. All the costs associated with the upgrading of the national AFIS, in scenario 3B, are related to the one-off costs (i.e. software licenses and development costs). Specifically, development costs for upgrading the national AFIS in scenario 3B, are the most significant costs incurred by Member States[58]. Also in this scenario, the one-off costs and the recurring costs are higher for the 28 Member States compared to what is incurred by the European Union.

Table 17 presents a consolidated view on the one-off and recurring costs incurred by the European Union and 28 Member States for the implementation of Scenario 3B.

[58] The estimated costs related to each cost item is further detailed into cost types (i.e. software, hardware, development, maintenance, support and training) in Annex 6.

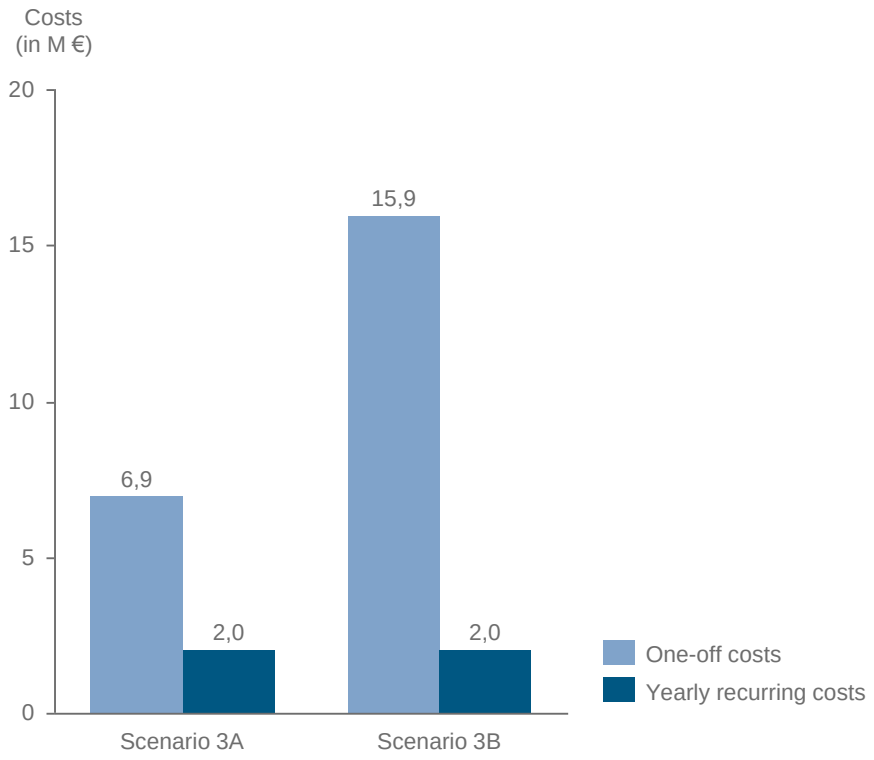
Table 17 Scenario 3B: Total costs summary (Fingerprints)

Estimated costs (*in thousand EUR*)	One-off costs	Recurring costs (Yearly)
Scenario 3B		
European Union	3,414	755
Member States	12,488	1,260
Total	**15,902**	**2,015**

Source: KURT SALMON Data Analysis, April 2016.

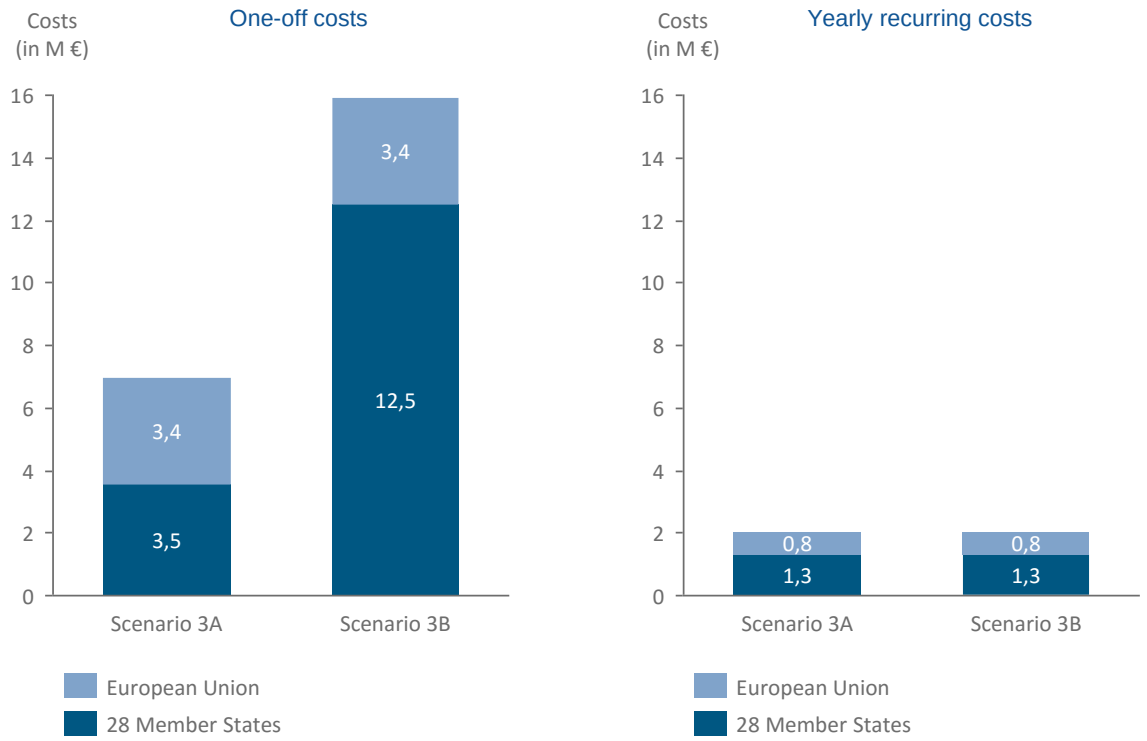
Finally, Figure 52 and Figure 53 present the comparison between Scenarios 3A and 3B in terms of total cost (one-off and recurring) as well as their distribution to the European Union and the 28 Member States.

Figure 52 Scenario 3A & 3B: Total costs for Fingerprints (1/2)



The difference between Scenarios 3A and 3B is the manual verification of fingerprints in the case of Scenario 3A and the automated verification of fingerprints in the case of Scenario 3B.

Figure 53 Scenario 3A & 3B: Total costs for Fingerprints (2/2)



7.2.5 Cost assessment of Scenarios 4A & 4B

This section provides a qualitative description, assumptions and quantitative cost estimations related to the cost items comprising Scenario 4A and 4B. This information is presented as follows:

- Table 18 presents a tabular view of qualitative descriptions, assumptions and quantitative cost estimates per cost item and per stakeholder group (European Union and Member States) related to Scenario 4A;
- Table 19 presents a summary of the quantitative cost estimates related to Scenario 4A detailing the break-down into type of costs (one-off and recurring).
- Table 20 presents a tabular view of qualitative descriptions, assumptions and quantitative cost estimates per cost item and per stakeholder group (European Union and Member States) related to Scenario 4B;
- Table 21 presents a summary of the quantitative cost estimates related to Scenario 4B detailing the break-down into type of costs (one-off and recurring).
- Figure 54 and Figure 55 present a graphical view of the quantitative cost estimates (one-off and recurring) per stakeholder group (European Union and Member States) for both Scenarios 4A and 4B;

Scenario 4A and Scenario 3A are the same with regards to fingerprints, the difference between these scenarios relates to the implementation of the alphanumeric part of the ECRIS TCN system. The same applies to Scenarios 4B and 3B.

Table 18 Scenario 4A: Cost elements

Stakeholder group	Scenario 4A Cost element	One-off	Recurring (Yearly)	Total Costs
Costs for the European Union	**Technical specification for an ECRIS TCN system** • **Description:** This cost item consists of the development of the technical specifications (documentation) for an ECRIS TCN system. The technical specifications aim at guiding the overall implementation of the ECRIS TCN system in Member States. The cost related to the technical specifications varies according to the number and complexity of the technical interfaces that need to be specified. For this scenario the specifications would include: ○ Specification of the technical interfaces for integration of the ECRIS TCN system at national level with ECRIS and CRR; ○ Specifications for integration with central AFIS for providing input, searches and central storage of FP files; ○ Specification of the technical interface for automated distributed "hit/no hit" search queries with other Member States (for alphanumeric data). • **Assumptions:** Maintenance of the technical specifications is assumed to be included in the overall maintenance of the ECRIS project.	186		186
	Update of the ECRIS technical specifications • **Description**: This cost item consists of the update the technical specification (documentation) of ECRIS in order to accommodate the changes added due to the new ECRIS TCN system components. These technical specifications are documents that enable Member States to implement their own implementation of ECRIS. • **Assumptions:** Maintenance of the technical specifications is assumed to be included in the overall maintenance of the ECRIS project.	88		88
	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 ECRIS TCN system components and ECRIS TCN principles (one-to-many communication). • **Assumptions:** Maintenance of the ECRIS RI is assumed to be included in the overall maintenance of the ECRIS project.	259		259
	Development of the ECRIS TCN system Reference Implementation • **Description:** This cost item consists of the development of the software component for ECRIS TCN system. The cost related to the development of the ECRIS TCN Reference Implementation varies according to the number and complexity of the software components to be developed. This scenario would include: ○ Technical interfaces for integration of the ECRIS TCN system at national level with the CRR and with ECRIS. ○ Technical interface for automated distributed "hit/no hit" search queries with Member States (alphanumeric data). ○ Technical interface with the central AFIS. ○ Integrated matching mechanism for performing queries on TCN using FP (integration with central AFIS) and alphanumeric data. ○ Application for sending updates on inclusion/removal of FP file to the central AFIS. ○ TCN fingerprint storage. • **Assumptions**: The following is assumed: ○ Member States will be able to use the Reference Implementation. ○ Additional cost on opting for a national implementation is not a cost mandated by the legislation.	931	186	1,117
	Set up of central AFIS system • **Description:** This cost item consists of the complete implementation of a centralised AFIS system at EU level managed by a European Institution or Agency (e.g. eu-LISA). • **Assumptions:** The estimated costs are based on the assumption that the central AFIS system would be able to cope with up to 3.5 thousand searches per day and 2.1 Tb of storage as expected in the ECRIS TCN system and detailed in Annex 3.	1,950	458	2,408
	Training on the use of fingerprints functionalities of ECRIS TCN system • **Description:** Training of officials using ECRIS to search using fingerprints. **Assumptions:** Training 2 trainers of each National Competent Authority		111	111
	Total costs: European Union (in thousand EUR)	**3,414**	**755**	**4,170**

Stakeholder group	Scenario 4A Cost element	One-off	Recurring (Yearly)	Total Costs
Costs for Member States	**Set up the ECRIS TCN system at national level for querying a central AFIS** • **Description:** This cost item consists of implementing and configuring the ECRIS TCN system Reference Implementation at national level. This includes: ○ Installing the ECRIS TCN system Reference Implementation in the Member States premises; ○ Connecting the ECRIS TCN system with the CRR and ECRIS RI. ○ Connecting the ECRIS TCN system with the central AFIS. • **Assumptions:** The following is assumed: ○ The integration of ECRIS TCN system in the national workflow for uploading FP into the ECRIS TCN system is excluded from the cost assessment. ○ No incremental cost on the network is incurred given that ECRIS is already using sTESTA. ○ It is assumed that the Reference Implementation can reuse hardware and server licenses from the ECRIS project, therefore no incremental cost for software and hardware is accounted.	3,500	1,260	4,760
	Total costs: Member States (in thousand EUR)	**3,500**	**1,260**	**4,760**
	Total costs: European Union and Member States *(in thousand EUR)*	**6,914**	**2,015**	**8,930**

Source: KURT SALMON Data Analysis, April 2016.

As in Scenario 3A, the total cost to implement Scenario 4A is EUR 8.9 million including one-off costs (i.e. initial investment) and recurring costs (i.e. one year operating costs). Approximately 53% of the total costs relates to the setting up the ECRIS TCN system at national level for querying a central AFIS, which is incurred by Member States. The costs associated with the setting up the ECRIS TCN system, in scenario 4A, are mostly related to the development costs for implementing and configuring the ECRIS TCN system (EUR 3.5 million)[59]. The one-off cost and the recurring costs are slightly higher for the 28 Member States compared to what is incurred by the European Union. Table 19 presents a consolidated view on the one-off and recurring costs incurred by the European Union and the 28 Member States for the implementation of Scenario 4A.

Table 19 Scenario 4A: Total costs summary (Fingerprints)

Estimated costs (*in thousand EUR*)	One-off costs	Recurring costs (Yearly)
Scenario 4A		
European Union	3,414	755
Member States	3,500	1,260
Total	**6,914**	**2,015**

Source: KURT SALMON Data Analysis, April 2016.

Both Scenarios 4A and 4B are based on a central AFIS managed by eu-LISA with an automated "hit/no hit" search with TCN FP (without ID data). Like in scenarios 3A and 3B, the difference between Scenarios 4A and 4B is that in Scenario 4A the verification of FP is performed without the support of an AFIS at national level, and in Scenario 4B the verification of FP is performed with support of an existing AFIS. Table 20 presents in detail the cost elements composing Scenario 4B.

[59] The estimated costs related to each cost item is further detailed into cost types (i.e. software, hardware, development, maintenance, support and training) in Annex 6.

Table 20 Scenario 4B: Cost elements

Stakeholder group	Scenario 4B Cost element	One-off	Recurring (Yearly)	Total Costs
Costs for the European Union	**Technical specification for an ECRIS TCN system** • **Description:** This cost item consists of the development of the technical specifications (documentation) for an ECRIS TCN system. The technical specifications aim at guiding the overall implementation of the ECRIS TCN system in Member States. The cost related to the technical specifications varies according to the number and complexity of the technical interfaces that need to be specified. For this scenario the specifications would include: ○ Specification of the technical interfaces for integration of the ECRIS TCN system at national level with ECRIS and CRR; ○ Specifications for integration with central AFIS for providing input, searches and central storage of FP files; ○ Specification of the technical interface for automated distributed "hit/no hit" search queries with other Member States (for alphanumeric data). • **Assumptions:** Maintenance of the technical specifications is assumed to be included in the overall maintenance of the ECRIS project.	186		186
	Update of the ECRIS technical specifications • **Description**: This cost item consists of the update of the technical specification (documentation) of ECRIS in order to accommodate the changes added due to the new ECRIS TCN system components. These technical specifications are documents that enable Member States to implement their own implementation of ECRIS. • **Assumptions:** Maintenance of the technical specifications is assumed to be included in the overall maintenance of the ECRIS project.	88		88
	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 ECRIS TCN system components and ECRIS TCN principles (one-to-many communication). • **Assumptions:** Maintenance of the ECRIS RI is assumed to be included in the overall maintenance of the ECRIS project.	259		259
	Development of the ECRIS TCN system Reference Implementation • **Description:** This cost item consists of the development of the software component for ECRIS TCN system. The cost related to the development of the ECRIS TCN Reference Implementation varies according to the number and complexity of the software components to be developed. This scenario would include: ○ Technical interfaces for integration of the ECRIS TCN system at national level with the CRR and with ECRIS. ○ Technical interface for automated distributed "hit/no hit" search queries with Member States (alphanumeric data). ○ Technical interface with the central AFIS. ○ Integrated matching mechanism for performing queries on TCN using FP (integration with central AFIS) and alphanumeric data. ○ Application for sending updates on inclusion/removal of FP file to the central AFIS. • **Assumptions**: The following is assumed: ○ Member States will be able to use the Reference Implementation. ○ Additional cost on opting for a national implementation is not a cost mandated by the legislation.	931	186	1,117
	Set up of central AFIS system • **Description:** This cost item consists of the complete implementation of a centralised AFIS system at EU level managed by a European Institution or Agency (e.g. eu-LISA). • **Assumptions:** The estimated costs are based on the assumption that the central AFIS system would be able to cope with up to 3.5 thousand searches per day and 2.1 Tb of storage as expected in the ECRIS TCN system and detailed in Annex 3.	1,950	458	2,408
	Training on the use of fingerprints functionalities of ECRIS TCN system • **Description:** Training of officials using ECRIS to search using fingerprints. **Assumptions:** Training 2 trainers of each National Competent Authority		111	111
	Total costs: European Union (in thousand EUR)	**3,414**	**755**	**4,170**

Stakeholder group	Scenario 4B Cost element	One-off	Recurring (Yearly)	Total Costs
Costs for Member States	**Set up the ECRIS TCN system at national level for querying a central AFIS** • **Description:** This cost item consists of implementing and configuring the ECRIS TCN system Reference Implementation at national level. This includes: ○ Installing the ECRIS TCN system Reference Implementation in the Member States premises; ○ Connecting the ECRIS TCN System with an existing AFIS ○ Connecting the ECRIS TCN system with the CRR and ECRIS RI. ○ Connecting the ECRIS TCN system with the central AFIS. • **Assumptions:** The following is assumed: ○ The integration of ECRIS TCN system in the national workflow for uploading FP into the central ECRIS TCN system is excluded from the cost assessment. ○ No incremental cost on the network is incurred given that ECRIS is already using sTESTA. ○ It is assumed that the Reference Implementation can reuse hardware and server licenses from the ECRIS project, therefore no incremental cost for software and hardware is accounted.	3,500	1,260	4,760
	Upgrade National AFIS for verification following a query in the central AFIS • **Description:** In case of a "hit", upon a request of a Member State, the requested Member State might decide to perform a verification based on fingerprints transmitted with the request. In this scenario it is assumed that the requested Member States will use the national AFIS to perform the verification process. Therefore this cost item includes the incremental development and software costs for upgrading the national AFIS to accommodate the requirements of verifying TCN fingerprints following a "hit/no hit" search query at the central AFIS. • **Assumptions:** The following is assumed: • No incremental hardware, maintenance and support due to the reuse of existing AFIS.	8,988		8,988
	Total costs: Member States (in thousand EUR)	12,488	1,260	13,748
	Total costs: European Union and Member States *(in thousand EUR)*	**15,902**	**2,015**	**17,917**

Source: KURT SALMON Data Analysis, April 2016.

Identical to Scenario 3B, the total cost to implement Scenario 4B is EUR 17.9 million including one-off costs (i.e. initial investment) and recurring costs (i.e. one year operating costs). Approximately 50% of the total costs relates to the upgrade of the National AFIS for verification following a search in the central AFIS. Therefore the one-off cost and the recurring costs are higher for the 28 Member States compared to what is incurred by the European Union. Table 21 presents a consolidated view on the one-off and recurring costs incurred by the European Union and 28 Member States for the implementation of Scenario 4B.

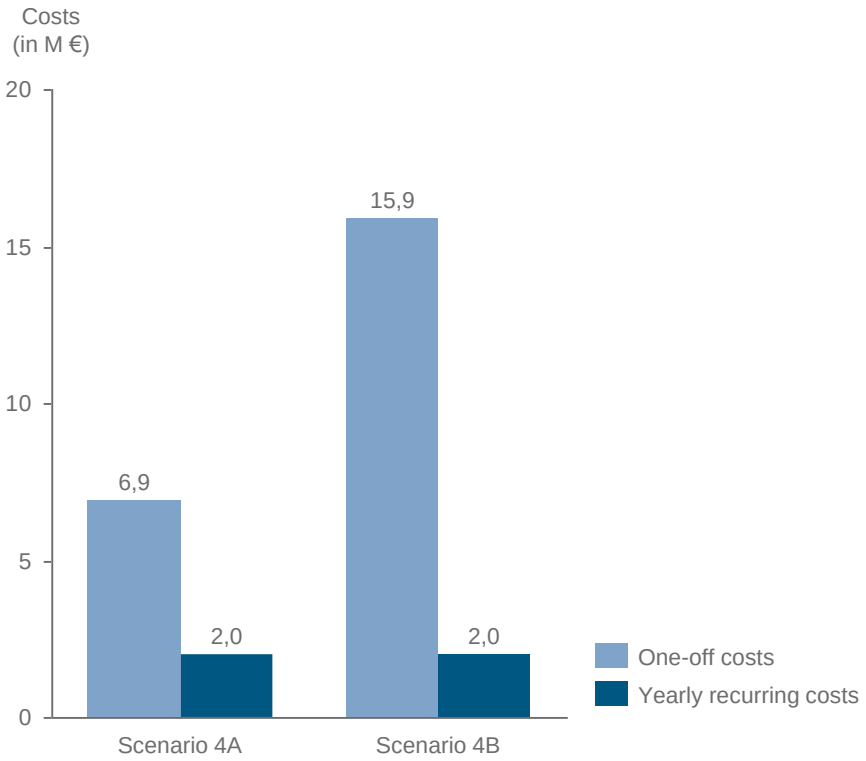
Table 21 Scenario 4B: Total costs summary (Fingerprints)

Estimated costs *(in thousand EUR)*	One-off costs	Recurring costs (Yearly)
Scenario 4B		
European Union	3,414	755
Member States	12,488	1,260
Total	**15,902**	**2,015**

Source: KURT SALMON Data Analysis, April 2016.

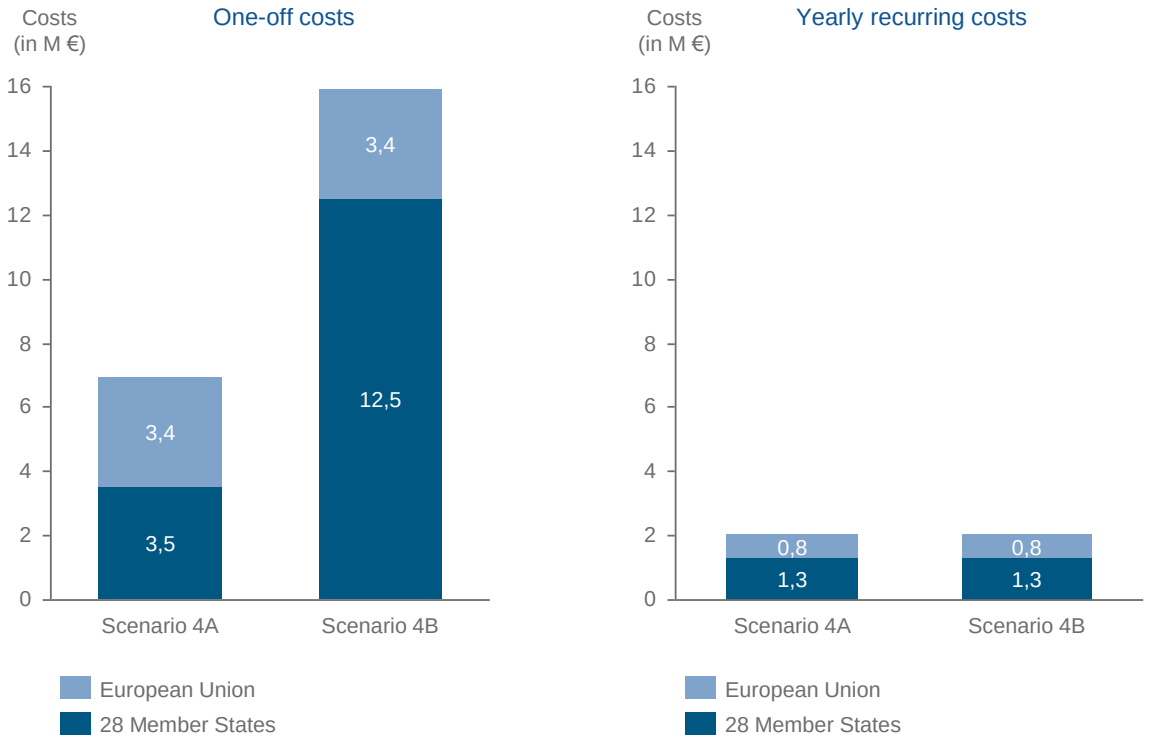
Finally, Figure 54 and Figure 55 present the comparison between Scenarios 4A and 4B in terms of total costs (one-off and recurring), as well as their distribution to the European Union and the 28 Member States.

Figure 54 Scenario 4A & 4B: Total costs for Fingerprints (1/2)



The difference between Scenarios 4A and 4B relates to the verification of fingerprints. In the case of Scenario 4A the verification is performed without the support of a national AFIS, while in the case of Scenario 4B the verification is performed with support of a national AFIS.

Figure 55 Scenario 4A & 4B: Total costs for Fingerprints (2/2)



7.3 Comparison of the costs for implementation of the technical scenarios

This section compares the costs associated with the technical scenarios for the implementation of the ECRIS TCN system. At first, it presents the comparison of costs for the inclusion of pseudonymised fingerprints in the ECRIS TCN exchanges (section 7.3.1) and then presents the consolidated comparison of the costs associated to the inclusion of pseudonymised fingerprints **and** alphanumeric data in the ECRIS TCN exchanges. The section focuses on presenting the costs incurred by each stakeholder group[60]; the European Union and the 28 Member States as well as per type of cost; one-off and yearly recurring costs.

7.3.1 Cost comparison for the inclusion of pseudonymised fingerprints

Based on the assessment of the technical scenarios for the inclusion of pseudonymised fingerprints in the ECRIS TCN system (section 7.2), Figure 56 and Figure 57 present the comparison of the eight technical scenarios in terms of total one-off and yearly recurring costs incurred by the European Union and by the 28 Member States.

The comparison of the scenarios assessed with regard to costs shows that the decentralised options (i.e. Scenario 1 and Scenario 2) are more costly than the centralised options (Scenario 3 and Scenario 4). This is the case because the implementation of Scenario 1 and Scenario 2 requires that an AFIS system is available **in each Member State** to support decentralised “hit/no hit” searches using fingerprints. On the other hand, in scenarios 3 and 4, the central AFIS supports the “hit/no hit” searches using fingerprints.

The comparison of the variants of the decentralised options shows that the variants A are more costly to implement than variants B. This is the case because the implementation of Scenarios 1A and 2A requires the setup of a new AFIS dedicated to ECRIS TCN exchanges; while the implementation of Scenarios 1B and 2B foresees the reuse of an existing national AFIS. The cost of setting up a new AFIS is significantly higher than upgrading an existing national AFIS. The difference in the costs of setting up a dedicated AFIS in Scenario 1A and 2A and upgrading a national AFIS in Scenarios 1B and 2B is related to the different requirements with regards to processing capacity and storage as well as to the complexity of the solution that needs to be put in place (impact on development costs).

With regard to the centralised options, the cost comparison shows that the implementation of variants B (i.e. Scenario 3B and 4B) is more costly than the implementation of the variants A (i.e. Scenarios 3A and 4A). This is the case because in the variants B the upgrading of the national AFIS for supporting the verification process following a positive hit search is foreseen (further detailed in sections 6.3 and 6.4). This cost item is not foreseen in scenarios 3A and 4A when the verification process is performed without the support of an AFIS system.

[60] Detailed view on the costs incurred by each Member State is presented in Annex 2 and detailed view per category of cost (software, hardware, development, maintenance, support and training) is presented in Annex 6.

Figure 56 Cost comparison for Fingerprints for EU and 28 MS (1/2)

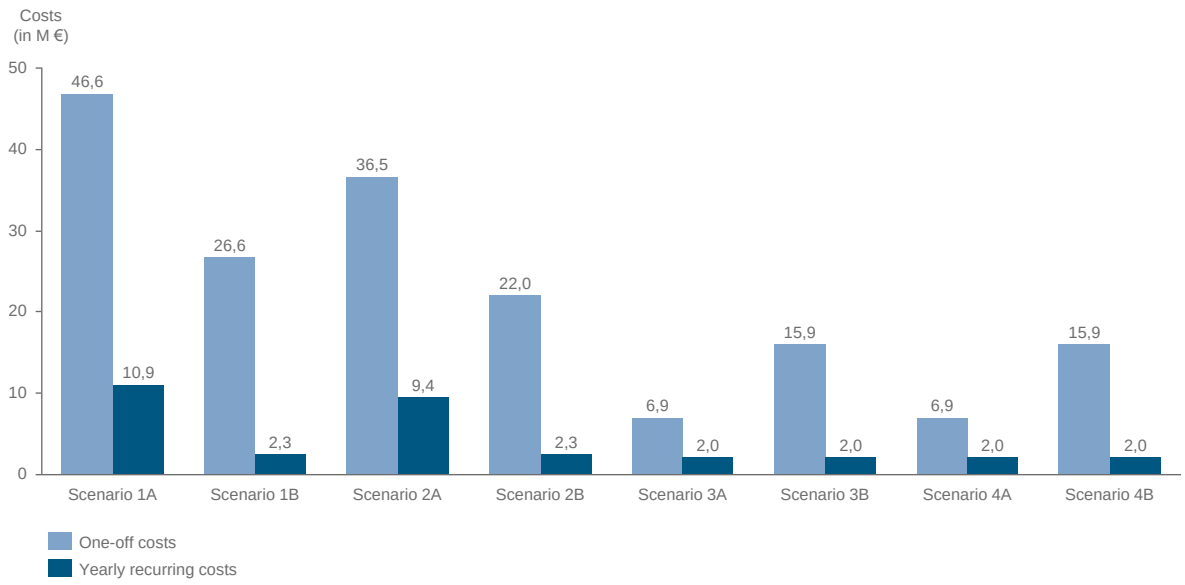
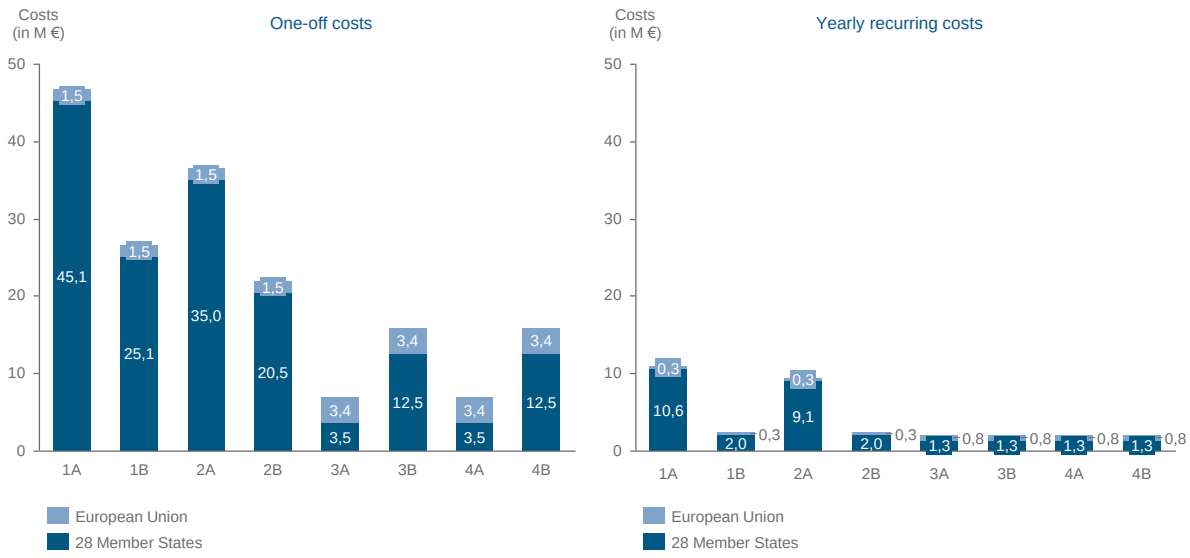


Figure 57 Cost comparison for Fingerprints for EU and 28 MS (2/2)

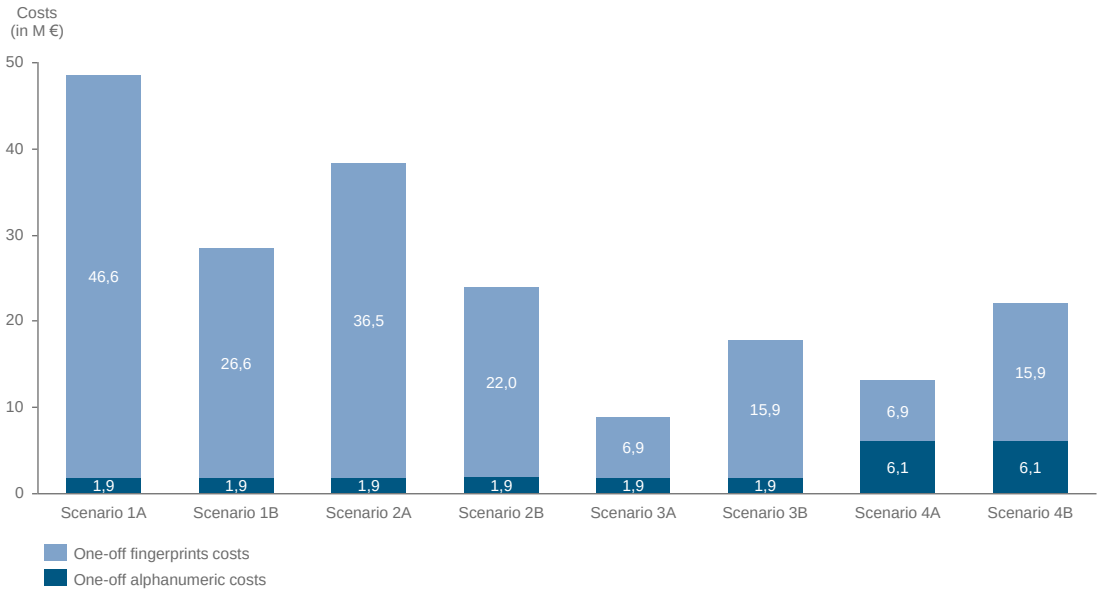


7.3.2 Cost comparison for the inclusion of pseudonymised fingerprints and alphanumeric data

Considering the description of each technical scenario as presented in section 6, the ECRIS TCN system consists of two main elements: the pseudonymised fingerprints and the alphanumeric data exchange. Therefore the total costs for implementing each scenario analysed includes the cost for implementing both fingerprints and alphanumeric elements. While the costs for the fingerprint element are extensively discussed in section 7.2, the costs for implementing the alphanumeric part are provided by the Assessment of ICT

impacts of the legislative proposal for ECRIS TCN performed by KURT SALMON in 2015[61]. Figure 58 and Figure 59 present a consolidated view of the comparison of the costs for implementation of the alphanumeric and fingerprint elements of the ECRIS TCN system.

Figure 58 Cost comparison for Fingerprints and Alphanumeric Data for the EU and 28 MS (1/3)



The costs for the implementation of the alphanumeric element in Scenarios 1A, 1B, 2A, 2B, 3A and 3B are identically estimated at EUR 1.9 million one-off and approximately EUR 0.9 million yearly recurring costs, as these scenarios foresee an identical implementation of the alphanumeric element in a decentralised way (e.g. reuse of the Mat3ch technology). Similarly, in scenarios 4A and 4B, the costs for the implementation of the alphanumeric element are estimated at approximately EUR 6.1 million one-off and at approximately EUR 1.7 million yearly recurring, by taking into account that these scenarios foresee the implementation of the alphanumeric implementation centrally.

The costs for implementation of the decentralised alphanumeric element are lower than for the centralised alphanumeric element, even if a decentralised approach means the deployment of 28 independent systems (one in each Member State). There are two main reasons for this cost difference. The first one is the reuse of an existing technology (Ma3tch) for the decentralised alphanumerical implementation. The use of this technology reduces costs due to the low complexity, low technical requirements and low cost for customisation of the existing tool to fit the ECRIS TCN system. The second one is that in the centralised implementation of the alphanumeric element, the technical requirements for high availability together with the processing power and storage capacity to serve the 28 Member States make it a more complex IT system.

[61] 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. Available at: http://ec.europa.eu/justice/criminal/files/ecris_tcn_ict_impact_assessment_final_report_en.pdf

Figure 59 Costs' comparison for Fingerprints and Alphanumeric Data for the EU and 28 MS (2/3)

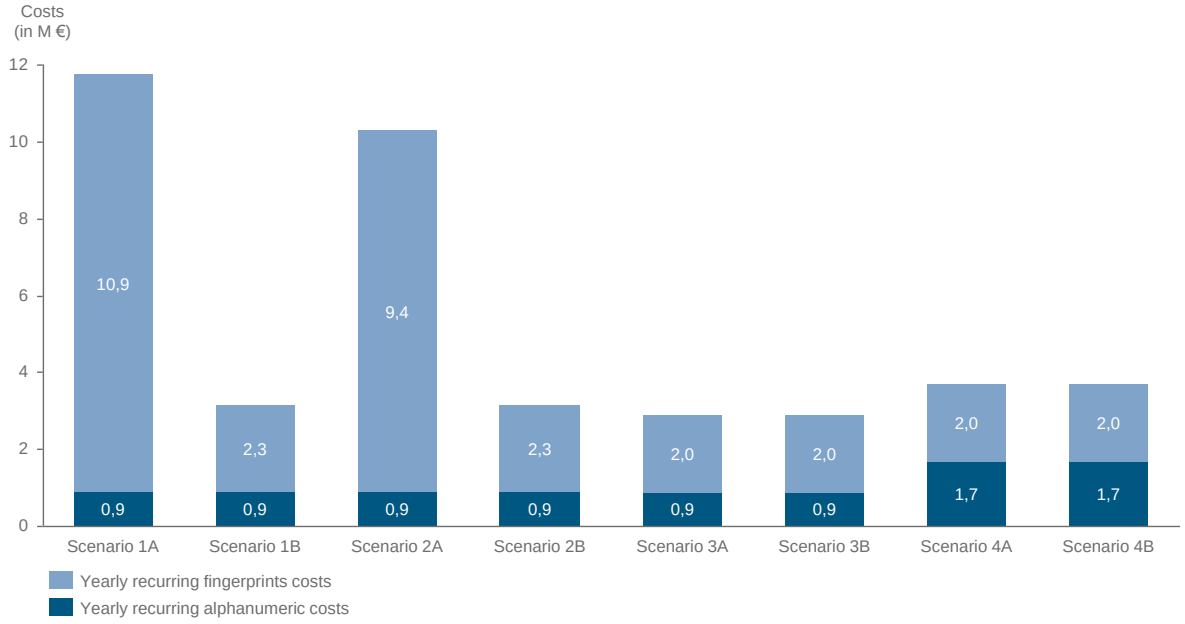
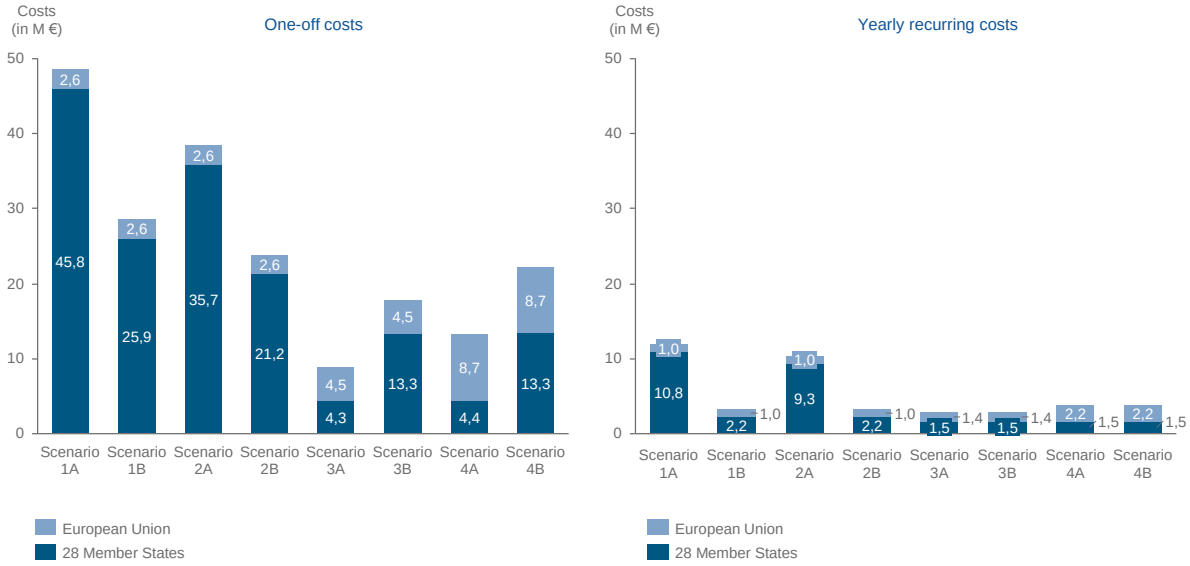


Figure 60 presents the comparison of the costs for the implementation of both alphanumeric and fingerprint elements focusing on the costs incurred by the European Union and 28 Member States for all scenarios.

Figure 60 Cost comparison for Fingerprints and Alphanumeric Data for the EU and 28 MS (3/3)



8 Conclusions

This section presents the conclusions of the ICT Cost Assessment on the inclusion of pseudonymised fingerprints in ECRIS TCN exchanges. The conclusions drawn in this ICT Cost Assessment follow the "**Least Cost Analysis"** method as specified in the Better Regulation Toolbox[62]. According to the method, the identified technical scenarios are assessed against the incurred incremental costs for their implementation. Subsequently each scenario is ranked. Table 22 shows the **results of** the cost assessed of each assessed technical scenario, using a score **ranking** from ● (lowest cost) to ●● ●● ●● ●● (highest cost).

Table 22 Overall evaluation of ECRIS TCN Technical Scenarios

Assessed technical scenarios	Total Costs *(in EUR)*	Efficiency *("least-costly")*
Scenario 1A	**60,221,306**	●● ●● ●● ●●
Fingerprints	57,492,785	
Alphanumeric	2,728,521	
Scenario 1B	**31,625,506**	●● ●● ●●
Fingerprints	28,896,985	
Alphanumeric	2,728,521	
Scenario 2A	**48,617,106**	●● ●● ●● ●
Fingerprints	45,888,585	
Alphanumeric	2,728,521	
Scenario 2B	**26,956,706**	●● ●● ●
Fingerprints	24,228,185	
Alphanumeric	2,728,521	
Scenario 3A	**11,658,127**	●
Fingerprints	8,929,606	
Alphanumeric	2,728,521	
Scenario 3B	**20,645,927**	●● ●
Fingerprints	17,917,406	
Alphanumeric	2,728,521	
Scenario 4A	**16,737,203**	●●
Fingerprints	8,929,606	
Alphanumeric	7,807,597	
Scenario 4B	**25,725,003**	●● ●●
Fingerprints	17,917,406	
Alphanumeric	7,807,597	

Source: KURT SALMON Data Analysis, April 2016.

[62] Better Regulation Toolbox, complementing SWD(2015) 111 final, Commission Staff Working Document, Better Regulation Guidelines, {COM(2015) 215 final} {SWD(2015) 110 final}, Strasbourg, 19.5.2015.

As a result, Scenario 3A is evaluated as least costly scenario to implement the ECRIS TCN system followed by Scenario 4A, while Scenario 1A and 2A are considered as most costly.

The least costly scenario to implement the ECRIS TCN system is Scenario 3A. The cost for implementation of Scenario 3A by Member States is estimated at EUR 5.7 million (one-off and one year recurring costs), compared with EUR 56.6 million for the highest cost Scenario 1A. For the European Union, the cost of implementing Scenario 3A is estimated at EUR 5.9 million (one-off and one year recurring costs), compared with EUR 3.5 million for Scenario 1A.

Overall, based on the technical, operational and cost assessments, the centralised scenarios 3 and 4 are better evaluated for the implementation of a fully automated system for exchanging pseudonymised fingerprints of convicted TCN (i.e. ECRIS TCN system). The centralised options are not only less costly but also potentially less complex to implement compared to the decentralised options. In evaluating the complexity of the different options, the main consideration was that the implementation of the ECRIS TCN system could benefit from using proven technologies and successful implementations of already existing and comparable fully automated centralised systems (e.g. EURODAC and VIS). The decentralised options are also considered feasible for the implementation of ECRIS TCN exchanges, however at higher costs and complexity than the centralised options.

9 Annexes

Annex 1. Administrative costs

As defined in the better regulation guidelines of the European Commission, administrative costs[63] are calculated on the basis of the average cost of the required administrative activity multiplied by the total number of activities (frequency) performed per year. The costs are estimated by multiplying a tariff (based on the average labour cost per hour in each Member State) [64] and the duration required per activity.

The following sections detail each of the elements needed for the calculation of the costs related to the administrative activities, introduced by the ECRIS TCN exchanges, and explain the methodology for the calculation of the administrative costs.

It is important to note that only the incremental (i.e. non-business as usual) costs for complying with regulation (i.e. enabling ECRIS TCN exchanges) are considered in scope of this study.

General assumptions

Administrative tasks costs are calculated for 28 Member states. The following general assumptions were made:

- The average number of TCN convictions per Member State is used as a frequency for some administrative tasks. The numbers were based on information collected through questionnaires submitted in 2010, 2012, 2014 and 2015[66]. Where data was not submitted, estimates were calculated on the basis of Member State TCN population.
- The labour cost rate per Member Sates used is the one established by Eurostat[64];
- With regards to the duration of human intervention, the data was collected from Member States[65]. When the collected data corresponded to a range; for example between 5 and 10 minutes, the maximum value of the range was used (e.g. 10 minutes). Where data was not available or not provided, the median value from the provided answers was used.

Administrative activities performed for the ECRIS TCN exchanges

Table 23 presents the identified administrative activities performed for the ECRIS TCN exchanges and details the duration and frequency related to these tasks.

[63] Since 2006, the Commission has been working to reduce the regulatory burdens (e.g. reporting and monitoring) created by EU legislation – making administrative processes easier and more efficient for citizens and businesses. More details on the Standard Cost Model to apply is to found here: http://ec.europa.eu/smart-regulation/refit/admin_burden/scm_en.htm
[64] Eurostat's structural earnings survey for occupation group ISCO 3 (Technicians and associate professionals), 2010.
[65] Data collected via on-line survey addressed to Member States during July 2015.

It must be noted that the cost related to the acquisition of fingerprints is out of scope of the current study. It is assumed that all Member States have a well-established process of acquiring high quality fingerprints of convicted TCN[66].

Table 23 Administrative activities performed for the ECRIS TCN exchanges

Administrative activity	Duration	Frequency
Storing incoming information or updating existing information on TCN convictions in the national criminal records system	The duration of this activity is the average **time** for human intervention needed for storing or updating information on **TCN convictions** in the national criminal record system. The values used for the duration of this activity were provided by Member States.	Every time a TCN is convicted the information on the new conviction should be stored in the national criminal records system. Therefore, it is assumed that the frequency of this activity is equal to **the average number of TCN convictions in each Member State** (total of 28 Member States)
Searching for a convicted TCN on the ECRIS TCN system using alphanumeric data and/or fingerprints	The duration of this activity is the average **time** for human intervention necessary for performing a search query in the ECRIS TCN system using alphanumeric data (e.g. name, gender, date of birth, etc.) and/or fingerprint images. This also includes the average time needed for fine tuning the search results per TCN searched. The value used for the duration of this activity is based on a conservative assumption of 15 minutes.	When ECRIS started operating, the search for past convictions increased gradually over the years. This was confirmed by ECRIS statistics. Assuming a similar approach for TCN than for ECRIS, it's reasonable to consider that the number of searches for past convictions for TCN will gradually increase over the years starting from **30% of the volume of TCN convictions up to 100% of the volume of TCN convictions** at maximum in normal operations.
Sending a request to other Member State through ECRIS	The duration of this activity is the average time for human intervention needed for sending a request to other Member States via ECRIS following positive "hit" results in the ECRIS TCN system. The values used for the duration of this activity were provided by Member States.	Based on ECRIS statistics, 30% of responses to requests contain one or more convictions. A similar percentage of positive responses is assumed for TCN requests. It means that a search for TCN convictions would yield a positive response match in 30% of the searches. Searches for a TCN with past convictions can lead to several matches. Assuming that TCN users would narrow down searches, or the calculation of the cost of administrative activities, it is assumed that an average of 4 matches are returned in each positive "hit" (30% of conviction). Therefore it is estimated that the frequency of sending requests via ECRIS are equal to **120% of the average number of TCN convictions** (4 matches * 30% of TCN convictions).

[66] Please refer to section 7.2.1 General assumptions.

Administrative activity	Duration	Frequency
Fingerprints verification	The duration of this activity is the average time for human intervention when verifying whether a fingerprint received in an ECRIS request corresponds to a fingerprint linked to a conviction in the receiving Member States. The values used for the duration of this activity were provided by fingerprints experts trained and certified to perform fingerprints verification. For the verification of fingerprints supported by an AFIS system the value of 5 minutes was used. For the verification of fingerprints without an AFIS system the duration of 10 minutes was used.	Following the same rationale used for the searches for a convicted TCN, it is assumed that the use of fingerprints when searching for a convicted TCN will gradually increase over time. It is assumed that the volume of ECRIS requests including fingerprints, which need to be individually verified, will vary from initial **30% up to 100% of the sent ECRIS requests at maximum in normal operations.**
Replying to a request from another Member State following a positive "hit" in the ECRIS TCN system	The duration of this activity is the average time for human intervention when replying to a requested from another Member State following a positive "hit" in the ECRIS TCN system The values used for the duration of this activity were provided by Member States.	Following the ECRIS principles, each request sent via ECRIS is answered, even if there are no past criminal record convictions. Subsequently, the number of replies is equal to the number of requests made in ECRIS. In the absence of statistics, the number of ECRIS requests sent by each Member State is used as a proxy indicator of the numbers of replies sent by each Member State. Even if the ratio of request/reply is not one-to-one, the number of replies should be proportional to the number of TCN convictions in a Member State.

Detailed calculation

This section presents the calculation of the cost related to the administrative activities performed for the ECRIS TCN exchanges. Table 24 below, provides in detail the range of values used for the calculation of the costs for each Member State.

Table 24 Frequency and duration of the administrative activities

Applies to / Administrative activity	Scenarios 1A, 1B, 2A, 2B, 3B. 4B (verification of fingerprints with support of an AFIS)		Scenarios 3A, 4A (verification of fingerprints without support of an AFIS)	
	Frequency of the task	Duration (in minutes)	Frequency of the task	Duration (in minutes)
Storing incoming information or updating existing information on TCN convictions in the national criminal records system	= Number of TCN convictions	0 -20 (as provided by Member States)	= Number of TCN convictions	0-20 (as provided by Member States)
Searching for a convicted TCN on the ECRIS TCN system using alphanumeric data and/or fingerprints	= Number of TCN convictions	15	= Number of TCN convictions	15

Applies to / Administrative activity	Scenarios 1A, 1B, 2A, 2B, 3B. 4B (verification of fingerprints with support of an AFIS)		Scenarios 3A, 4A (verification of fingerprints without support of an AFIS)	
	Frequency of the task	Duration (in minutes)	Frequency of the task	Duration (in minutes)
Sending a request to other Member State through ECRIS	=120% of TCN convictions	0 – 10 (as provided by Member States)	=120% of TCN convictions	0 – 10 (as provided by Member States)
Fingerprints verification	= 30% to 100% of requests sent through ECRIS	5	= 30% to 100% of requests sent through ECRIS	10
Replying to a request from another Member State following a positive "hit" in the ECRIS TCN system	=120% of TCN convictions	10 – 180 (as provided by Member States)	120% of TCN convictions	10 – 180 (as provided by Member States)

As mentioned in section 5.1.1 and also highlighted in the Impact Assessment[13] it is reasonable to consider that the number of searches using the ECRIS TCN system will gradually increase over the years. As shown in Table 25, the total administrative costs for each of scenarios 1A, 1B, 2A, 2B, 3B and 4B, are estimated at approximately EUR 4.6 million, which represents in average EUR 0.1 million per year per Member State when the exchanges will start (30% of TCN convictions are searched). The total administrative costs are approximately EUR 13.9 million, which represents in average EUR 0.5 million per year per Member State, when the system is at maximum capacity in normal operation (100% of TCN convictions are searched).

Table 25 Administrative costs of ECRIS TCN for Scenario 1A, 1B, 2A, 2B, 3B, and 4B

Member State	30% of TCN Convictions are Searched *(cost in EUR per year)*	100% of TCN Convictions are Searched *(cost in EUR per year)*
AT	56,000	164,000
BE	178,000	520,000
BG	2,000	6,000
CY	8,000	22,000
CZ	5,000	14,000
DE	1,170,000	4,521,000
DK	173,000	353,000
EE	35,000	113,000
EL	110,000	319,000
ES	211,000	594,000
FI	5,000	20,000
FR	762,000	2,220,000
HR	2,000	5,000
HU	20,000	59,000
IE	74,000	191,000

Member State	30% of TCN Convictions are Searched *(cost in EUR per year)*	100% of TCN Convictions are Searched *(cost in EUR per year)*
IT	406,000	1,184,000
LT	1,000	1,000
LU	96,000	265,000
LV	200	700
MT	1,000	4,000
NL	469,000	1,001,000
PL	11,000	29,000
PT	41,000	121,000
RO	1,000	2,000
SE	105,000	300,000
SI	46,000	157,000
SK	2,000	5,000
UK	589,000	1,718,000
Total (in EUR)	**4,600,000**	**13,900,000**
Average (in EUR)	**160,000**	**500,000**

Source: KURT SALMON Data Analysis, April 2016.

Figure 61 and Figure 62 below visualise respectively the administrative costs for Scenarios 1A, 1B, 2A, 2B, 3B, and 4B when 30% and 100% of the TCN convictions are searched.

Figure 61 Administrative costs for Scenarios 1A, 1B, 2A, 2B, 3B, and 4B (30% searches)

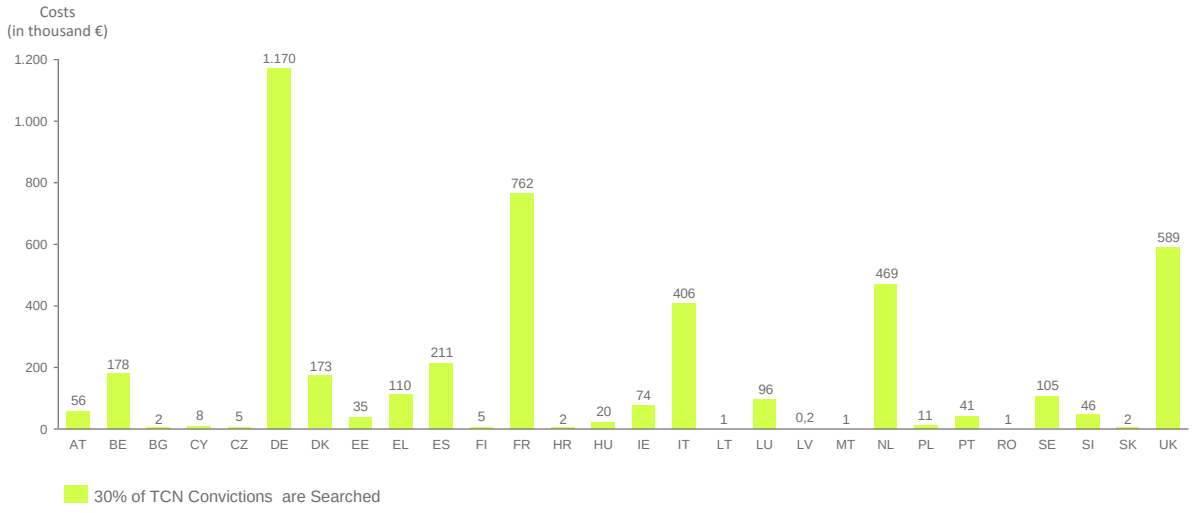
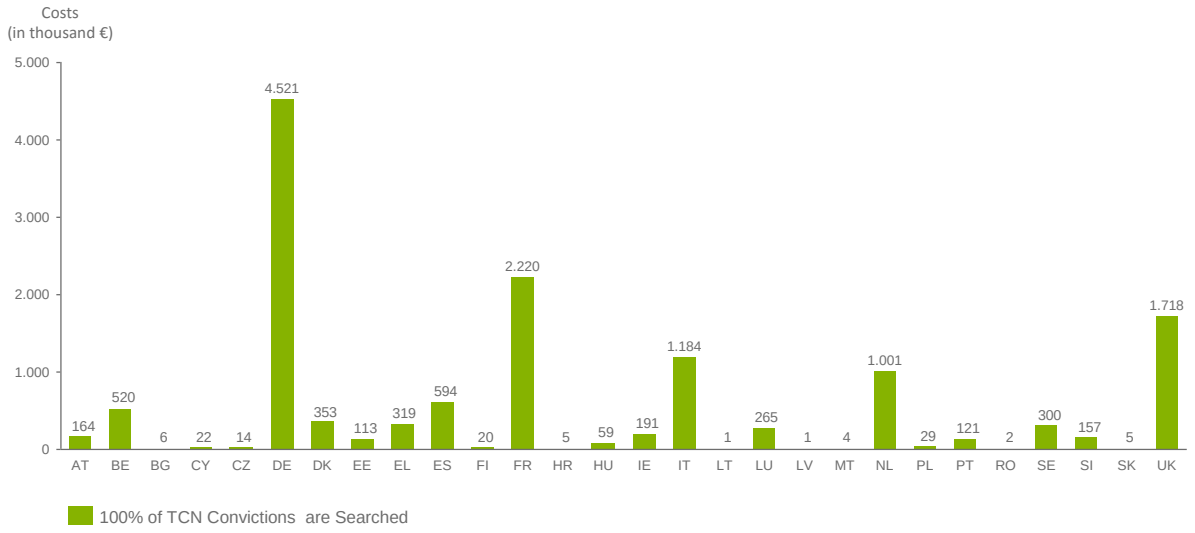


Figure 62 Administrative costs for Scenarios 1A, 1B, 2A, 2B, 3B, and 4B (100% searches)



Based on the description of the technical scenarios (Section 6), Scenarios 3A and 4A perform verification of FP without the support of an AFIS, which increases the estimated time for calculation of the verification task (10 minutes for verification without support of an AFIS and 5 minutes for verification supported by an AFIS). Therefore, as shown in Table 26 below, the administrative costs for Scenarios 3A and 4A are higher compared to Scenarios 1A, 1B, 2A, 3B and 4B. At the start (30% searches) the administrative costs for Scenarios 3A and 4A are estimated at approximately EUR 4.7 million, averaging at EUR 0.1 per year per Member State. In normal operation (100% searches) the administrative costs are approximately EUR 15.9 million, averaging at EUR 0.5 million per year per Member State.

Table 26 Administrative costs of ECRIS TCN for Scenario 3A and 4A

Member State	30% of TCN Convictions are Searched *(cost in EUR per year)*	100% of TCN Convictions are Searched *(cost in EUR per year)*
AT	57,000	186,000
BE	185,000	591,000
BG	2,000	6,000
CY	8,000	25,000
CZ	5,000	17,000
DE	1,230,000	5,217,000
DK	175,000	385,000
EE	35,000	117,000
EL	113,000	363,000
ES	220,000	694,000
FI	5,000	24,000
FR	788,000	2,523,000
HR	2,000	5,000
HU	21,000	67,000
IE	75,000	210,000
IT	420,000	1,346,000
LT	1,000	2,000

Member State	30% of TCN Convictions are Searched *(cost in EUR per year)*	100% of TCN Convictions are Searched *(cost in EUR per year)*
LU	100,000	315,000
LV	200	800
MT	1,000	4,000
NL	479,000	1,115,000
PL	11,000	33,000
PT	43,000	137,000
RO	1,000	2,000
SE	110,000	348,000
SI	46,000	160,000
SK	2,000	6,000
UK	610,000	1,952,000
Total (in EUR)	**4,700,000**	**15,900,000**
Average (in EUR)	**170,000**	**570,000**

Source: KURT SALMON Data Analysis, April 2016.

Figure 63 and Figure 64 below visualise respectively the administrative costs for Scenarios 3A and 4A when 30% and 100% of the TCN convictions are searched.

Figure 63 Administrative costs for Scenario 3A and 4A (30% searches)

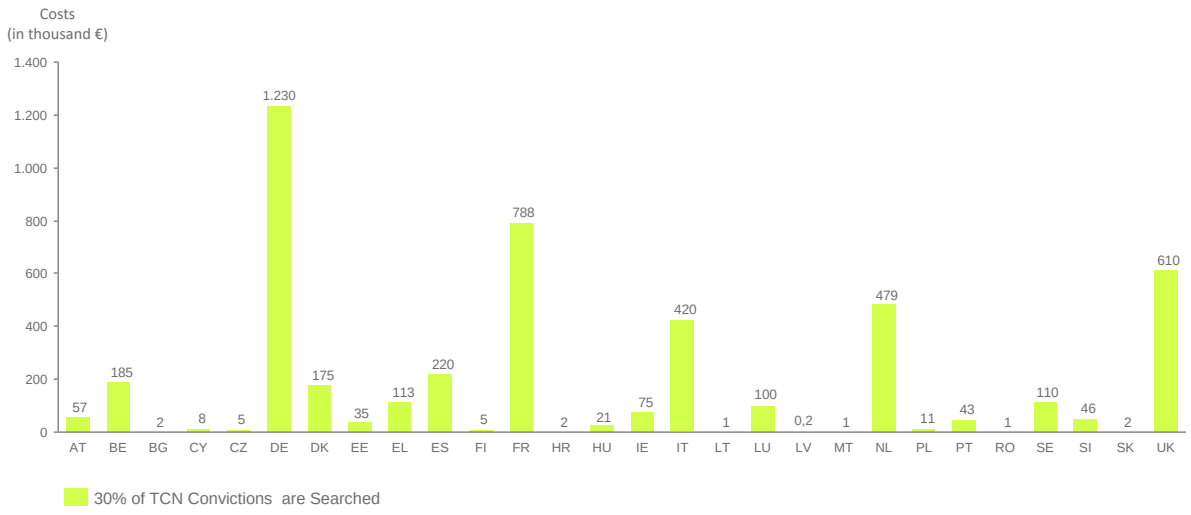


Figure 64 Administrative costs for Scenario 3A and 4A (100% searches)

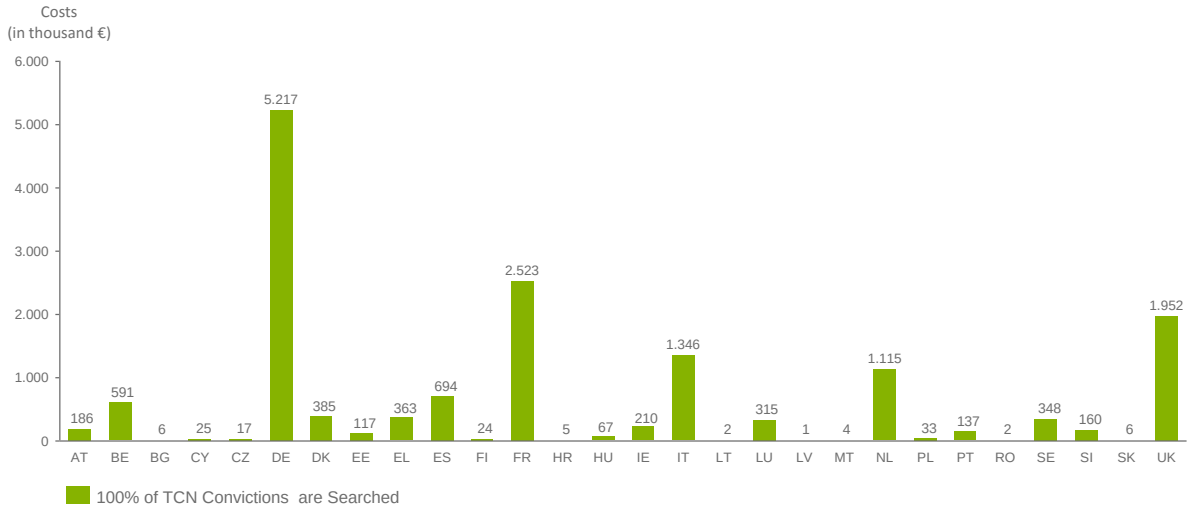
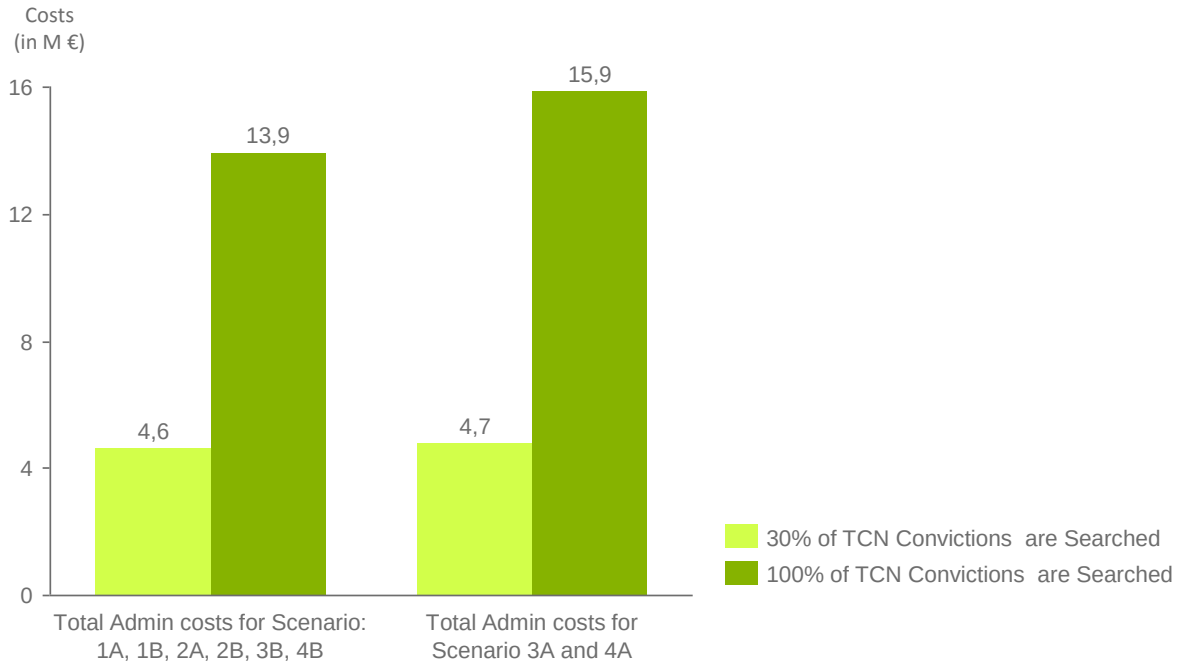


Figure 65 below visualises the total administrative costs per year for all scenarios for the implementation and operation of the ECRIS TCN system, when 30% of TCN convictions are searched and when the system is used in its full capacity (100% of TCN convictions are searched). Administrative costs for Scenarios 3A and 4A are higher compared to the other scenarios, due to the fact that a manual verification of FP upon an ECRIS request is performed.

Figure 65 Total Administrative costs per year



Annex 2. Distribution of cost per Member State

Based on the yearly volume of convictions (see general assessment assumptions presented in section 7.2.1), Table 27 presents the type of producer of TCN convictions. The grouping of Member States was used for estimating the necessary storage capacity and volume of matching operations and subsequently the associated costs of the following items:

- **Setup of a dedicated AFIS system to support the ECRIS TCN system** in scenarios 1A and 2A;
- **Upgrade of a national AFIS** in scenarios 1B, 2B, 3B and 4B;
- **Set up the ECRIS TCN system** in all scenarios (1A, 1B, 2A, 2B, 3A, 3B, 4A and 4B).

Table 27 Member States categorised according to the number of TCN convictions per year

Number of TCN convictions/year	Member States								Type of producer of TCN convictions
500	MT	HR	SK	BG	RO	LT	LV	EE	Low
5,000	CZ	SI	IE	CY					
10,000	PT	AT	FI	PL					
20,000	EL	HU	BE	LU	DK	SE			Medium
50,000	ES	IT	NL						
90,000	FR	UK							
270,000	DE								High

Figure 66 and Figure 67 present the one-off and yearly recurring costs incurred per Member State depending on the number of TCN convictions per year.

Figure 66 One-off costs per Member State for fingerprints according to the number of TCN convictions/year

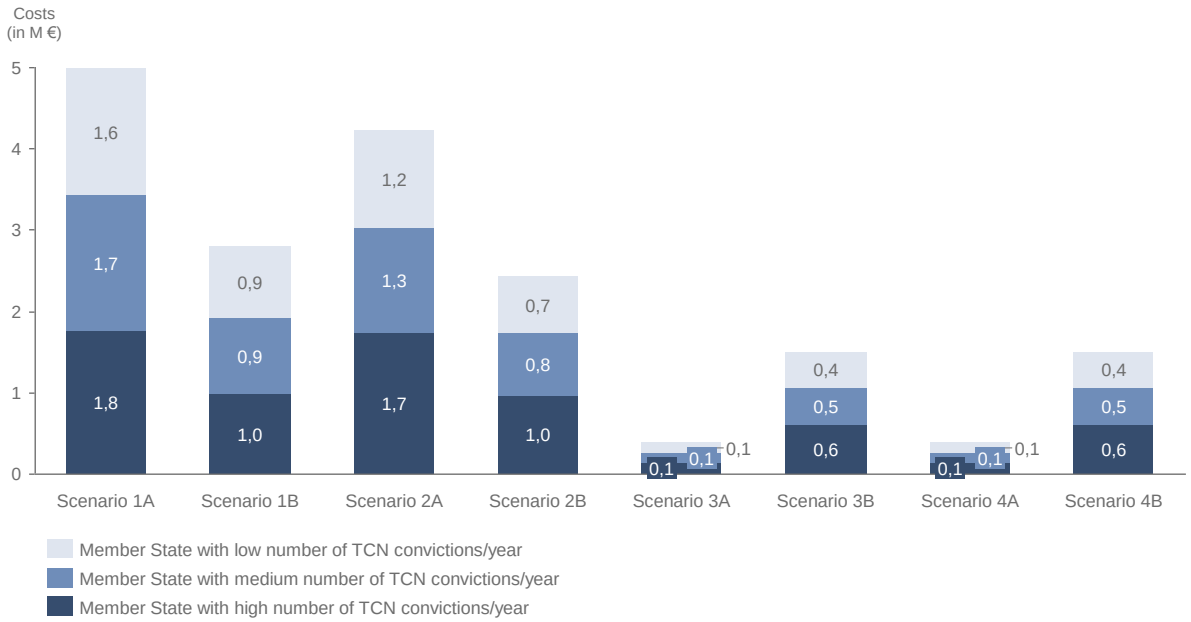


Figure 67 Yearly recurring costs per Member State for fingerprints according to the number of TCN convictions/year

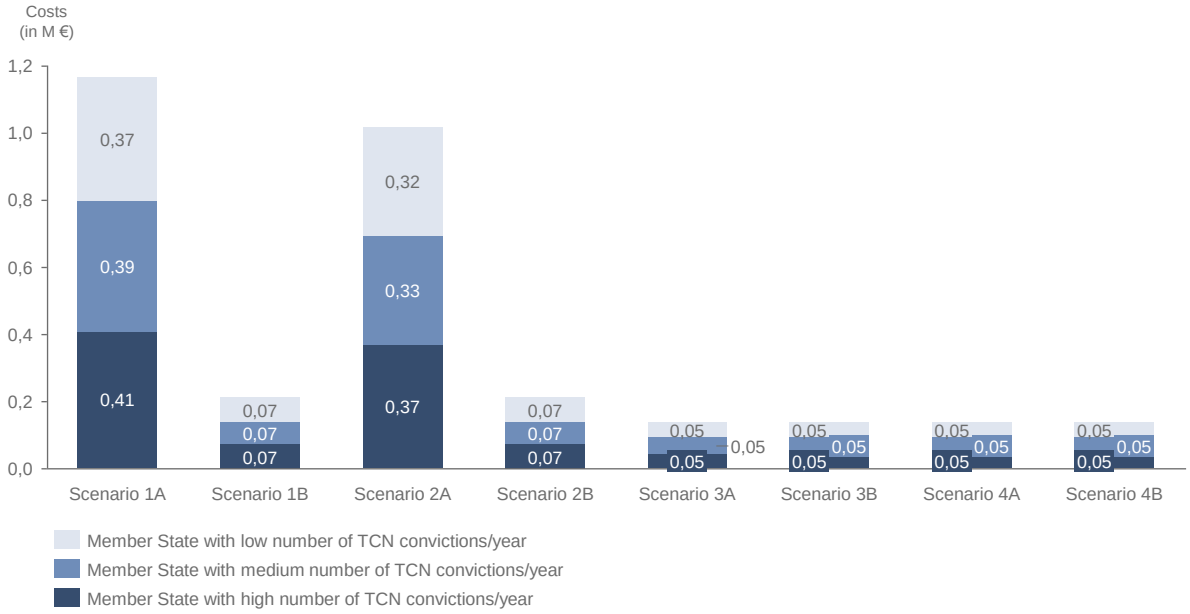


Figure 68 and Figure 69 present the cost for the alphanumeric exchanges in all scenarios assessed based on the Assessment of ICT impacts of the legislative proposal for ECRIS TCN performed by KURT SALMON in 2015[67]. Figure 68 presents the costs incurred by Member States in scenarios 1, 2 and 3 where alphanumeric data is exchanged in a decentralised fashion using Ma3tch technology. Figure 69 presents the costs incurred by Member States in scenario 4 where the alphanumeric data is included and exchanged with the central system managed by a European Agency (e.g. eu-LISA).

[67] 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. Available at: http://ec.europa.eu/justice/criminal/files/ecris_tcn_ict_impact_assessment_final_report_en.pdf

Figure 68 Alphanumeric costs for Scenarios 1A, 1B, 2A, 2B, 3A, and 3B

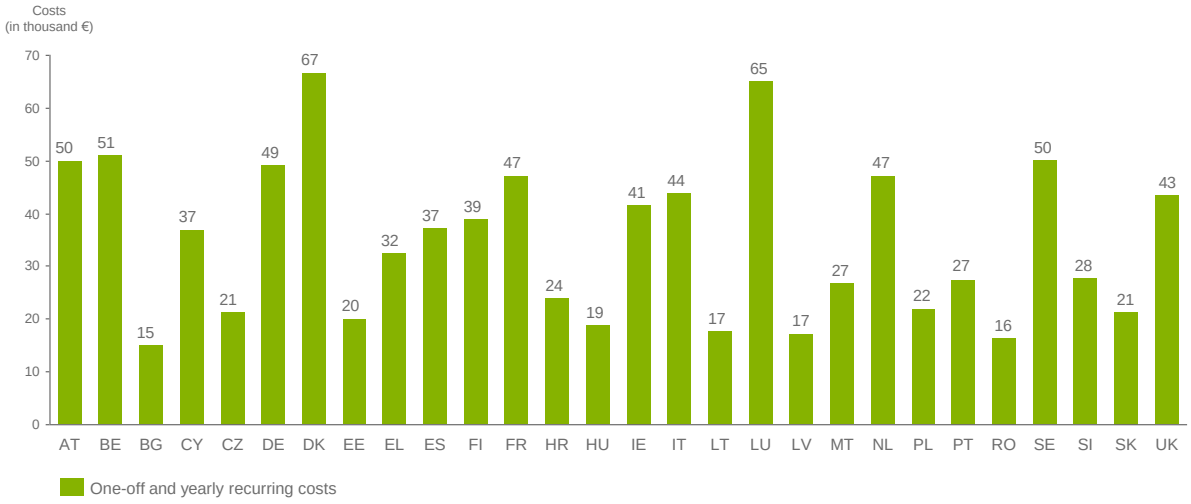
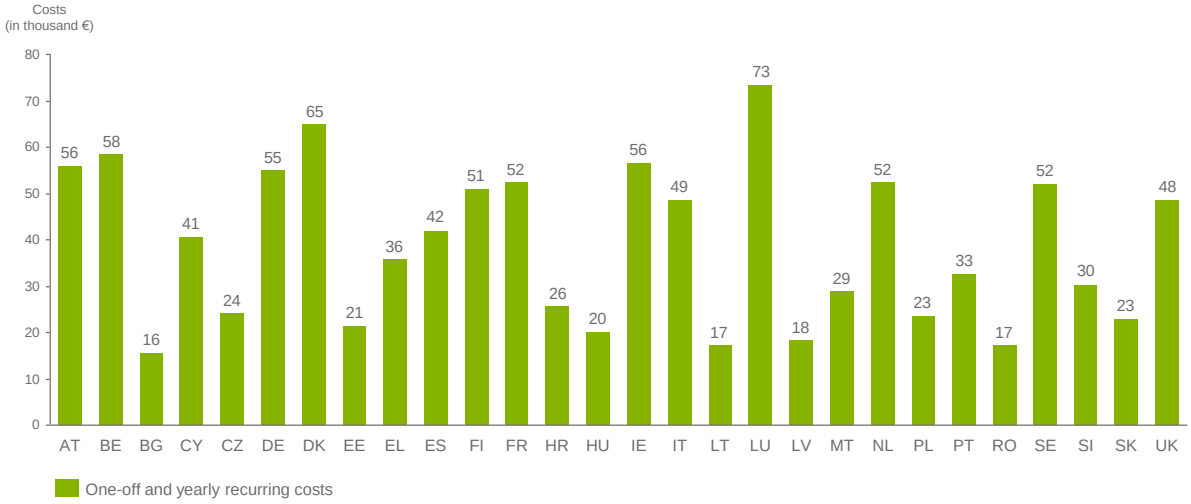


Figure 69 Alphanumeric costs for Scenarios 4A and 4B



Annex 3. Volumetric and fingerprints sizing information for the ECRIS TCN exchanges

This section presents volumetric and fingerprints sizing information that can be expected for the different scenario described in section 6. The estimated figures serve as requirements regarding the components handling digitalised fingerprint files (i.e. AFIS components). As confirmed by the vendors consulted in the context of this study[68], the number of processing operations (e.g. number of *one-to-many matching* operations) and storage capacity are the main parameters impacting the costs of an AFIS solution.

General assumptions on TCN fingerprint processing and storage

In order to calculate the estimates, a series of assumptions are made on the basis of the figures provided by the Member States for 2014, regarding convictions of TCN and on the basis of ECRIS statistics. Several figures are rounded up or maximised, in order to have a slightly more pessimistic view, catering for worst case situations.

- Highest amount of convictions of TCN per Member State: 270,000 per year (Germany)
    - To simulate a peak year in the calculations, 10% is added to this number (i.e. 297,000 per year)
- In average 700,000 convictions against TCN are handed down throughout the EU per year.
    - To simulate a peak year in the calculations, 10% is added to this number (i.e. 770,000 per year)
- For **all** TCN convictions, fingerprints are captured and entered into the 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 system. 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 ECRIS TCN system contain tenprints images with a high level of quality. The pseudonymised NIST files stored within the ECRIS TCN system or AFIS have been stripped and contain at most only 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 0.6 MB.
- In order to estimate the amount of ECRIS requests concerning TCN subjects, it is assumed that the same trends as for EU non-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 ECRIS notifications: 295,000 per year
        - On a yearly basis there are 17% more requests than new notifications (346,000/295,000). This percentage takes into account the fact that in practice

[68] More details on the data collection are presented in section 7.1.2.2.

there are slightly less requests for criminal proceedings issued on a yearly basis compared to the amount of new convictions (the ratio is not 1:1), but also the fact that a number of requests are also issued for purposes other than criminal proceedings.

- The volume of processing operations estimated in all the scenarios do not contain provisions for additional features that could be provided, such as running additional *one-to-many* matching operations for facilitating the verification of fingerprints by the central authorities of Member States when replying to ECRIS requests on TCN. In case such additional features are required and need to be implemented, it will be necessary to increase the estimated load for the TCN system so as to tailor its capacity appropriately.
- Depending on the scenarios and on the data exchange processes, some of the numbers estimated depend greatly on whether a given Member State is a high producer of TCN convictions. It is assumed that a Member State handing down a high number of convictions against TCN will also issue a high number of ECRIS requests relating to TCN. This assumption is reinforced by the fact that 80% of ECRIS requests are issued for the purpose of criminal proceedings, the vast majority thus occurring during the pre-trial stages.

In order to provide a means of comparison, three sizes are defined:

- **High:** Member States convicting in average between 90,000 and 270,000 TCN per year (using a maximum of 297,000 TCN per year for peak years)
- **Medium:** Member States convicting in average between 10,000 and 90,000 TCN per year (using a maximum of 99,000 TCN per year for peak years)
- **Low:** Member States convicting in average less than 10,000 TCN per year (using a maximum of 11,000 TCN per year for peak years)

Estimated volume of TCN fingerprint processing and storage

This section provides details on the estimated volumes for the data exchanges in ECRIS TCN. It focuses in particular on the IT component that needs to store and process the TCN fingerprints, this either being a dedicated AFIS (Scenarios 1A and 2A), an existing national AFIS (Scenarios 1B and 2B) or a central AFIS (Scenarios 3 and 4).

The estimated volume in the table below is global and independent of the implementation scenario chosen. This volume is extrapolated based on the current ECRIS trends and numbers, estimated for years with peak activity:

Table 28 Estimated number of ECRIS requests for TCN

Estimated volume		max/yearly
Estimated average number of ECRIS requests for TCN (EU-WIDE)	For purposes of criminal proceedings	696,000
	For other purposes	208,000
	Total	**904,000**
Estimated maximum number of ECRIS requests for TCN, issued by a HIGH convicting Member State	For purposes of criminal proceedings	269,000
	For other purposes	80,000
	Total	**349,000**
Estimated maximum number of ECRIS requests for TCN, issued by a MEDIUM convicting Member State	For purposes of criminal proceedings	89,000
	For other purposes	27,000
	Total	**116,000**
Estimated maximum number of ECRIS requests for TCN, issued by a LOW convicting Member State	For purposes of criminal proceedings	10,000
	For other purposes	3,000
	Total	**13,000**

The following sections present estimated volume, calculated and presented when relevant depending on each scenario:

- Number of input processing operations: this relates to the number of NIST files the AFIS component receives as input and needs to pseudonymise, transform and store
- Number of output operations: this relates to the number of NIST files that the AFIS needs to transform, encrypt and send via sTESTA to another Member State or to the central AFIS (i.e. how many dissemination operations need to be performed)
- Number of one-to-many matching operations: represents the number of one-to-many matching operations that need to be handled by the AFIS for responding to “hit/no hit” queries
- Storage: represents the total size of NIST files that need to be stored by the AFIS. This is an incremental number that grows in time as each year additional TCN fingerprints are captured and stored. A view on 5 years is provided in this section, where “year 1” corresponds to the first year of full operational usage of the ECRIS TCN system (assuming that the system is fully operational between first of January and the end of that year). It is also assumed that the ECRIS TCN system will be empty when starting up on its first day of operational usage as there is no obligation to prefill the system with identity information for past convictions of TCN.

Regarding the estimated volume for the storage of TCN FP files, it is expected that during the first years of operations of the ECRIS TCN system, the number of FP files to be stored steadily increases. However after several years of operations it can be expected that the volume stabilises as TCN convictions reach progressively their end of retention period. As a consequence, this means that after several years of operations, the addition of new fingerprint files in the ECRIS TCN system will also be counterbalanced by the removal of fingerprint files corresponding to convictions that have expired. However, this is not expected to occur during the first 5 years of operations. Furthermore no realistic numbers are available at this stage for evaluating correctly when and how many fingerprint files will be removed per year at average.

Estimated volume and storage of TCN fingerprints for Scenario 1

In Scenario 1, the figures are determined by the following key facts:

- Each Member State uses its own AFIS at national level for storing and processing the TCN fingerprints, either as a dedicated one embedded in the ECRIS TCN system as in Scenario 1A or a national AFIS that is extended and reused as in Scenario 1B.
- The TCN identity information – both fingerprints and alphanumeric data – are shared with all other Member States. This implies that the ECRIS TCN systems of all Member States are synchronised and contain the same amount and set of data.
- The "hit/no hit" search is performed fully at national level using the ECRIS TCN system of the requesting Member State. This implies that the Member States issuing a high number of ECRIS requests for TCN subjects, are also the ones performing high numbers of "hit/no hit" search operations. Inversely, Member States issuing only "low" amounts of ECRIS requests for TCN subjects, are only performing equivalently low amounts of "hit/no hit" searches.

The estimated volume expected for the technical component that stores and processes TCN fingerprints in Scenario 1 are presented in the tables below. The estimated number of processing operations depends on the number of TCN convictions in Member States[69] as presented in tables Table 29, Table 30 and Table 31, whereas the estimated storage volume is the same for all Member States as presented in Table 32. In the case of Scenario 1B that is based on the principle of extending and reusing an existing national AFIS, these numbers provide the additional load and storage required for the purpose of ECRIS TCN.

Table 29 Estimated number of processing operations – Scenario 1 (low)

Type of input processing operation	max/daily	max/yearly
Number of FP files entered by the CA (full NIST file used as input)	44	11,000
Number of FP files received as input from the ECRIS TCN system of other Member States	3,078	769,500
Number of FP files sent to the ECRIS TCN system of other Member States (i.e. dissemination)	44	11,000
Number of one-to-many matching operations	52	12,910

Table 30 Estimated number of processing operations – Scenario 1 (medium)

Type of input processing operation	max/daily	max/yearly
Number of FP files entered by the CA (full NIST file used as input)	396	99,000
Number of FP files received as input from the ECRIS TCN system of other Member States	3,044	760,999
Number of FP files sent to the ECRIS TCN system of other Member States (i.e. dissemination)	396	99,000
Number of one-to-many matching operations	465	116,189

[69] The categorisation of Member States according to the number of TCN convictions per year (low, medium, high) is presented in detail in Annex 2.

Table 31 Estimated number of processing operations – Scenario 1 (high)

Type of input processing operation	max/daily	max/yearly
Number of FP files entered by the CA (full NIST file used as input)	1,188	297,000
Number of FP files received as input from the ECRIS TCN system of other Member States	1,892	473,000
Number of FP files sent to the ECRIS TCN system of other Member States (i.e. dissemination)	1,188	297,000
Number of one-to-many matching operations	1,394	348,567

Table 32 Estimated volume for storage, cumulative over 5 years – Scenario 1 (all Member States)

Storage	Year 1	Year 2	Year 3	Year 4	Year 5
Number of TCN FP files stored (incremental per year)	700,000	1,400,000	2,100,000	2,800,000	3,500,000
Estimated disk space required (in TB)	0,42	0,84	1,26	1,68	2,1

Estimated volume and storage of TCN fingerprints for Scenario 2

In Scenario 2, the figures are determined by the following key facts:

- Each Member State uses its own AFIS at national level for storing and processing the TCN fingerprints, either as a dedicated one embedded in the ECRIS TCN system as in Scenario 2A or a national AFIS that is extended and reused as in Scenario 2B.
- The TCN fingerprints are not shared with all Member States, whereas the alphanumeric identity data is still shared. This implies that the ECRIS TCN system of each Member State only contains the set of TCN fingerprints corresponding to the amount of TCN convicted at national level.
- The “hit/no hit” search part that involves fingerprints is in a distributed manner. This implies that the Member States issuing a high number of ECRIS requests for TCN subjects, are also the ones sending a high amount of “hit/no hit” search operations to the other Member States. Inversely, Member States issuing only low amounts of ECRIS requests for TCN subjects are only sending few “hit/no hit” search queries to all other Member States but do receive the highest amount of such distributed “hit/ no hit” search queries.

The estimated volume expected for the technical component that stores and processes TCN fingerprints in Scenario 2 are presented in the tables below. The estimated number of processing operations (Table 33, Table 34 and Table 35) and the estimated storage volume (Table 36, Table 37 and Table 38) depend on the number of TCN convictions in Member States[70]. In the case of Scenario 2B that is based on the principle of extending and reusing an existing national AFIS, these numbers provide the additional load and storage required specifically for the purpose of ECRIS TCN.

[70] The categorisation of Member States according to the number of TCN convictions per year (low, medium, high) is presented in detail in Annex 2.

Table 33 Estimated number of processing operations – Scenario 2 (low)

Type of input processing operation	max/daily	max/yearly
Number of FP files entered by the CA (full NIST file used as input)	44	11,000
Number of FP files sent to the ECRIS TCN system of other Member States for launching a distributed "hit/no hit" search	52	12,910
Number of "hit/no hit" search queries sent to all other Member States (each FP is sent to 27 other Member States)	1,394	348,567
Number of one-to-many matching operations to perform (is equal to the number of "hit/no hit" search queries received from all other Member States)	3,563	890,783

Table 34 Estimated number of processing operations – Scenario 2 (medium)

Type of input processing operation	max/daily	max/yearly
Number of FP files entered by the CA (full NIST file used as input)	396	99,000
Number of FP files sent to the ECRIS TCN system of other Member States for launching a distributed "hit/no hit" search	465	116,189
Number of "hit/no hit" search queries sent to all other Member States (each FP is sent to 27 other Member States)	12,548	3,137,105
Number of one-to-many matching operations to perform (is equal to the number of "hit/no hit" search queries received from all other Member States)	3,150	787,504

Table 35 Estimated number of processing operations – Scenario 2 (high)

Type of input processing operation	max/daily	max/yearly
Number of FP files entered by the CA (full NIST file used as input)	1,188	297,000
Number of FP files sent to the ECRIS TCN system of other Member States for launching a distributed "hit/no hit" search	1,394	348,567
Number of "hit/no hit" search queries sent to all other Member States (each FP is sent to 27 other Member States)	37,645	9,411,314
Number of one-to-many matching operations to perform (is equal to the number of "hit/no hit" search queries received from all other Member States)	2,221	555,126

Table 36 Estimated volume for storage, cumulative over 5 years – Scenario 2 (low)

Storage	Year 1	Year 2	Year 3	Year 4	Year 5
Number of TCN FP files stored (incremental per year)	10,000	20,000	30,000	40,000	50,000
Estimated disk space required (in TB)	0,006	0,012	0,018	0,024	0,03

Table 37 Estimated volume for storage, cumulative over 5 years – Scenario 2 (medium)

Storage	Year 1	Year 2	Year 3	Year 4	Year 5
Number of TCN FP files stored (incremental per year)	90,000	180,000	270,000	360,000	450,000
Estimated disk space required (in TB)	0,05	0,10	0,16	0,21	0,27

Table 38 Estimated volume for storage, cumulative over 5 years – Scenario 2 (high)

Storage	Year 1	Year 2	Year 3	Year 4	Year 5
Number of TCN FP files stored (incremental per year)	270,000	540,000	810,000	1,080,000	1,350,000
Estimated disk space required (in TB)	0,16	0,32	0,49	0,65	0,81

It is interesting to note in this scenario that the estimated storage volume is not very significant compared to professional, large-scale IT solutions, as even in the highest cases less than 1TB will be required after 5 years.

However, in terms of processing fingerprint files, there is a significant difference between Member States that are convicting few TCN and those handing down many convictions. Indeed the AFIS component of "low" number of convictions, in comparison with "high" number of convictions, will need to process and store few fingerprint files but will need to support the highest amount of *one-to-many* matching operations per day.

Estimated volume and storage of TCN fingerprints for Scenarios 3 and 4

In the scenarios 3 and 4 which are based on a central architecture, volume need to be estimated for the ECRIS TCN system installed in each Member State but also for the AFIS managed by eu-LISA which centralises the TCN fingerprints. As this section only focuses on the volume associated for the processing, storage and transmission of fingerprints, without detailing the treatment of alphanumeric identity data, the numbers are the same for both scenarios.

As a reminder, in Scenarios 3A and 4A, the ECRIS TCN system installed in each Member State does not contain a fully-fledged AFIS component but a simple fingerprint processing and storage system. The numbers provided in this section apply to both situations.

The estimated volume expected for the technical component that stores and processes TCN fingerprints in the Member States are presented in the tables below. The estimated number of processing operations and the estimated storage volume depend on the size of the convicting Member State. In the cases of Scenarios 3B and 4B that are based on the principle of extending and reusing an existing national AFIS, these numbers provide the additional load and storage required specifically for the purpose of ECRIS TCN.

Table 39 Estimated number of processing operations (low)

Type of input processing operation	max/daily	max/yearly
Number of FP files entered by the CA (full NIST file used as input)	44	11,000
Number of FP files sent to the central AFIS for launching a "hit/no hit" search	52	12,910

Table 40 Estimated number of processing operations (medium)

Type of input processing operation	max/daily	max/yearly
Number of FP files entered by the CA (full NIST file used as input)	396	99,000
Number of FP files sent to the central AFIS for launching a "hit/no hit" search	465	116,189

Table 41 Estimated number of processing operations (high)

Type of input processing operation	max/daily	max/yearly
Number of FP files entered by the CA (full NIST file used as input)	1,188	297,000
Number of FP files sent to the central AFIS for launching a "hit/no hit" search	1,394	348,567

Table 42 Estimated volume for storage, cumulative over 5 years (low)

Storage	Year 1	Year 2	Year 3	Year 4	Year 5
Number of TCN FP files stored (incremental per year)	10,000	20,000	30,000	40,000	50,000
Estimated disk space required (in TB)	0,006	0,012	0,018	0,024	0,03

Table 43 Estimated volume for storage, cumulative over 5 years (medium)

Storage	Year 1	Year 2	Year 3	Year 4	Year 5
Number of TCN FP files stored (incremental per year)	90,000	180,000	270,000	360,000	450,000
Estimated disk space required (in TB)	0,05	0,10	0,16	0,21	0,27

Table 44 Estimated volume for storage, cumulative over 5 years (high)

Storage	Year 1	Year 2	Year 3	Year 4	Year 5
Number of TCN FP files stored (incremental per year)	270,000	540,000	810,000	1.080,000	1.350,000
Estimated disk space required (in TB)	0,16	0,32	0,49	0,65	0,81

Regarding the estimated volume for Member States, it is interesting to note that the load on the national ECRIS TCN system is now directly proportionate to the number convicted TCN and to the number of "hit/no hit" queries issued by the Member State. Thus "low" producers require less capacity and processing power than "high" producers.

The tables below present the estimated volume for the central AFIS managed by eu-LISA.

Table 45 Estimated number of processing operations (central AFIS)

Type of input processing operation	max/daily	max/yearly
Number of FP files received from all Member States (to process and store)	3,080	770,000
Number of one-to-many matching operations (triggered by all "hit/no hit" search queries from all Member States)	3,615	903,693

Table 46 Estimated volume for storage, cumulative over 5 years (central AFIS)

Storage	Year 1	Year 2	Year 3	Year 4	Year 5
Number of TCN FP files stored (incremental per year)	700,000	1,400,000	2,100,000	2,800,000	3,500,000
Estimated disk space required (in TB)	0,42	0,84	1,26	1,68	2,1

Regarding the central AFIS, the storage capacity estimated is not very significant for such a system. However, the central AFIS needs to have a high capacity for being able to process the reception of many fingerprint files per day and simultaneously execute many "hit/no hit" search queries per day. This

emphasises again the need to a fully automated process, without human intervention (i.e. in “lights-out” mode).

The figures presented here above were not used for the cost estimate of a central system. Instead, due to timing constraints, this study uses the volumetric estimated during the ICT Cost Assessment[71] conducted in 2015 and the associated costs as a proxy for the costs related to the Central AFIS foreseen in scenarios 3 and 4. The cost estimates were provided by eu-LISA in 2015 based on the following requirements:

- **Number of one-to-many matching operations (triggered by all “hit/no hit” search queries from all Member States):** 5,000 per day. This number is higher than the estimated requirements for the central AFIS of the ECRIS TCN system (max 3,615/day as shown in Table 45).

- **Number of FP files received from all Member States (to process and store):** 1,100 per day. This number is lower than the estimated requirements for the central AFIS of the ECRIS TCN system (max 3,080/day as shown in **Error! Reference source not found.**).

- **Estimated disk space required (in TB):** Starting at 30 TB in the first year and growing to 46TB after 5 years of operation. This is considerably higher than the estimated disk space needed for the central AFIS of the ECRIS TCN system (2.1 TB after 5 years operation as shown in Table 46).

[71] 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. Available at: http://ec.europa.eu/justice/criminal/files/ecris_tcn_ict_impact_assessment_final_report_en.pdf.

Annex 4.Country fiche on the State of play of Fingerprints usage

Below is a list of country fiches for each EU Member State, in which the state of play of fingerprints in the respective countries is analysed in-depth, based on questionnaires, existing literature and country visits (where applicable).

Table 47 Country Fiches on the State of Play of fingerprints usage

Member State	Country Fiche
Austria	AUSTRIA STATE OF PLAYv1.0.docx
Belgium	BELGIUM STATE OF PLAYv1.0 .docx
Bulgaria	BULGARIA STATE OF PLAYv1.0.docx
Croatia	CROATIA STATE OF PLAYv1.0.docx
Cyprus	CYPRUS STATE OF PLAYv1.0.doc
Czech Republic	CZECH_REPUBLIC_STATE_OF_PLAYv1.1.docx
Denmark	DENMARK STATE OF PLAYv1.0.docx
Estonia	ESTONIA STATE OF PLAYv1.0.docx

Member State	Country Fiche
Finland	FINLAND STATE OF PLAYv1.0.docx
France	FRANCE STATE OF PLAYv0.1.docx
Germany	GERMANY STATE OF PLAYv1.0.docx
Greece	GREECE STATE OF PLAYv0.1.docx
Hungary	HUNGARY STATE OF PLAYv1.0.docx
Ireland	IRELAND STATE OF PLAYv1.0.docx
Italy	ITALY STATE OF PLAYv1.0.docx
Latvia	LATVIA STATE OF PLAYv1.0.docx
Lithuania	LITHUANIA STATE OF PLAYv1.0.docx

Member State	Country Fiche
Luxembourg	LUXEMBOURG STATE OF PLAYv0.1.docx
Malta	MALTA STATE OF PLAYv1.0.docx
Poland	POLAND STATE OF PLAYv1.0.docx
Portugal	PORTUGAL STATE OF PLAYv1.0.docx
Romania	ROMANIA STATE OF PLAYv1.0.doc
Slovakia	SLOVAKIA STATE OF PLAYv1.0.docx
Slovenia	SLOVENIA STATE OF PLAYv0.1.docx
Spain	SPAIN STATE OF PLAYv1.0.docx
Sweden	SWEDEN STATE OF PLAYv1.0.docx

Member State	Country Fiche
The Netherlands	THE NETHERLANDS STATE OF PLAYv1.0.docx
United Kingdom	UNITED KINGDOM STATE OF PLAYv1.1.docx

Annex 5. Workshop on pseudonymisation of fingerprints – European Commission, Brussels, 15 March 2016

Welcome and Introduction

The European Commission welcomed all attendees and introduced the ECRIS TCN work and the objectives of the meeting. European Commission representatives introduced the ECRIS system and provided a historical and practical overview to all attendees.

The European Commission has commissioned a feasibility study to see if fingerprints could be used in the context of ECRIS TCN exchanges. There is a particular emphasis on “pseudonymisation”, especially in light of the proposed decentralised approach.

The European Commission stressed that the focus of the meeting should be on the feasibility of the technical aspects of searching TCN fingerprints in a pseudonymised, one-to-many context. The European Commission would like to explore whether there are any existing solutions in the market place or whether there are any research activities in this respect. There is a recognition that this is very innovative thinking and there may not be existing solutions that have been operationally deployed.

Existing pseudonymisation solutions / research activities

The AFIS vendors confirmed that there are no operational solutions in place, in terms of one-to-many fingerprint matching mechanisms. Although some research has been carried out in this field, this is predominantly focused on one-to-one matching mechanisms. With these solutions, there are some technical limitations in regards to scalability and accuracy, but also the impact on the existing systems in terms of system migration and overall performance.

The AFIS vendors confirmed that if something were to be developed in the context of one-to-many, it would be a very expensive undertaking, as this would require significant developmental work concerning system architecture and security.

No fingerprint system is 100% accurate and therefore careful consideration also needs to be given to determining the required accuracy and performance requirements for an ECRIS TCN AFIS. Such an initiative would be a frontrunner developmental project, with little past experience to build upon. There would be no guarantees that it would be possible to develop a suitably reliable AFIS to meet the ECRIS TCN requirements.

Conclusion

All AFIS vendors present at the meeting stated, that there are a number of commercially available template protection techniques to work in a variety of one-to-one verification scenarios. However, there are no existing market solutions for template protection (pseudonymisation) of fingerprints in one-to-many matching scenario.

Annex 6.Detailed view on the cost estimates

Table 48 and Table 49 present the estimated total costs in EUR incurred by the European Union and by the Member States, grouped by cost type (i.e. development, maintenance, support, hardware, software and training) for each of the technical scenarios for the inclusion of fingerprints.

Table 48 Cost distribution per type for the inclusion of Fingerprints in ECRIS TCN exchanges

Cost Type	Scenario	Cost incurred by	One-off *(in EUR)*	Recurring *(in EUR)*
Development	**TOTAL 1A**		**25,610,400**	
		EU	1,530,400	
		MS	24,080,000	
	TOTAL 1B		**18,760,400**	
		EU	1,512,400	
		MS	17,248,000	
	TOTAL 2A		**24,355,400**	
		EU	1,505,400	
		MS	22,850,000	
	TOTAL 2B		**17,994,400**	
		EU	1,484,400	
		MS	16,510,000	
	TOTAL 3A		**5,714,400**	
		EU	2,214,400	
		MS	3,500,000	
	TOTAL 3B		**12,054,400**	
		EU	2,214,400	
		MS	9,840,000	
	TOTAL 4A		**5,714,400**	
		EU	2,214,400	
		MS	3,500,000	
	TOTAL 4B		**12,054,400**	
		EU	2,214,400	
		MS	9,840,000	
Maintenance	**TOTAL 1A**			**9,651,200**
		EU		197,200
		MS		9,454,000
	TOTAL 1B			**1,594,800**
		EU		194,800
		MS		1,400,000
	TOTAL 2A			**8,176,000**
		EU		194,000
		MS		7,982,000
	TOTAL 2B			**1,591,400**
		EU		191,400
		MS		1,400,000
	TOTAL 3A			**1,024,271**
		EU		324,271
		MS		700,000
	TOTAL 3B			**1,024,271**
		EU		324,271
		MS		700,000
	TOTAL 4A			**1,024,271**

Cost Type	Scenario	Cost incurred by	One-off *(in EUR)*	Recurring *(in EUR)*
		EU		324,271
		MS		700,000
	TOTAL 4B			**1,024,271**
		EU		324,271
		MS		700,000
Support	**TOTAL 1A**			**1,120,000**
		MS		1,120,000
	TOTAL 1B			**560,000**
		MS		560,000
	TOTAL 2A			**1,120,000**
		MS		1,120,000
	TOTAL 2B			**560,000**
		MS		560,000
	TOTAL 3A			**640,250**
		EU		80,250
		MS		560,000
	TOTAL 3B			**640,250**
		EU		80,250
		MS		560,000
	TOTAL 4A			**640,250**
		EU		80,250
		MS		560,000
	TOTAL 4B			**640,250**
		EU		80,250
		MS		560,000
Hardware	**TOTAL 1A**		**7,882,000**	
		MS	7,882,000	
	TOTAL 1B			
		MS		
	TOTAL 2A		**5,507,000**	
		MS	5,507,000	
	TOTAL 2B			
		MS		
	TOTAL 3A		**1,200,000**	**240,000**
		EU	1,200,000	240,000
	TOTAL 3B		**1,200,000**	**240,000**
		EU	1,200,000	240,000
		MS		
	TOTAL 4A		**1,200,000**	**240,000**
		EU	200,000	240,000
	TOTAL 4B		**1,200,000**	**240,000**
		EU	1,200,000	240,000
		MS		
Software	**TOTAL 1A**		**13,118,500**	
		MS	13,118,500	
	TOTAL 1B		**7,871,100**	
		MS	7,871,100	
	TOTAL 2A		**6,619,500**	
		MS	6,619,500	

Cost Type	Scenario	Cost incurred by	One-off *(in EUR)*	Recurring *(in EUR)*
	TOTAL 2B		**3,971,700**	
		MS	3,971,700	
	TOTAL 3B		**2,647,800**	
		MS	2,647,800	
	TOTAL 4B		**2,647,800**	
		MS	2,647,800	
Training	**TOTAL 1A**			**110,685**
		EU		110,685
	TOTAL 1B			**110,685**
		EU		110,685
	TOTAL 2A			**110,685**
		EU		110,685
	TOTAL 2B			**110,685**
		EU		110,685
	TOTAL 3A			**110,685**
		EU		110,685
	TOTAL 3B			**110,685**
		EU		110,685
	TOTAL 4A			**110,685**
		EU		110,685
	TOTAL 4B			**110,685**
		EU		110,685

Source: KURT SALMON Data Analysis, April 2016.

Table 49 Cost distribution per cost element for the inclusion of Fingerprints in ECRIS TCN exchanges

Scenario	Cost element	One-off *(in EUR)*	Recurring *(in EUR)*
Scenario 1A	**Total Scenario 1A**	**46,610,900**	**10,881,885**
	Setup of a dedicated AFIS system to support the ECRIS TCN system	**38,080,500**	**8,614,000**
	• Development	17,080,000	
	• Hardware	7,882,000	
	• Maintenance		8,054,000
	• Support		560,000
	• Software	13,118,500	
	Set up the ECRIS TCN system for local query in the dedicated AFIS	**7,000,000**	**1,960,000**
	• Development	7,000,000	
	• Hardware		
	• Maintenance		1,400,000
	• Support		560,000
	• Software		
	Development of the ECRIS TCN system reference Implementation	**986,000**	**197,200**
	• Development	986,000	
	• Maintenance		197,200
	Update the ECRIS reference implementation	**259,200**	
	• Development	259,200	
	Technical specification for an ECRIS TCN system	**197,000**	
	• Development	197,000	
	Update of the ECRIS technical specifications	**88,200**	
	• Development	88,200	

Scenario	Cost element	One-off *(in EUR)*	Recurring *(in EUR)*
	Training personnel to collect fingerprints and search ECRIS using fingerprints		**110,685**
	• Training		110,685
Scenario 1B	**Total Scenario 1B**	**26,631,500**	**2,265,485**
	Upgrade National AFIS	**18,119,100**	
	• Development	10,248,000	
	• Hardware		
	• Software	7,871,100	
	Set up the ECRIS TCN system reference implementation for local query in the national AFIS	**7,000,000**	**1,960,000**
	• Development	7,000,000	
	• Hardware		
	• Maintenance		1,400,000
	• Support		560,000
	• Software		
	Development of the ECRIS TCN system reference Implementation for local queries in a national AFIS	**974,000**	**194,800**
	• Development	974,000	
	• Maintenance		194,800
	Update the ECRIS reference implementation	**259,200**	
	• Development	259,200	
	Technical specification for an ECRIS TCN system	**191,000**	
	• Development	191,000	
	Update of the ECRIS technical specifications	**88,200**	
	• Development	88,200	
	Training personnel to collect fingerprints and search ECRIS using fingerprints		**110,685**
	• Training		110,685
Scenario 2A	**Total Scenario 2A**	**36,481,900**	**9,406,685**
	Setup of a dedicated AFIS system to support the ECRIS TCN system	**27,976,500**	**7,142,000**
	• Development	15,850,000	
	• Hardware	5,507,000	
	• Maintenance		6,582,000
	• Support		560,000
	• Software	6,619,500	
	Set up the ECRIS TCN system for distributed hit/no hit search queries in dedicated AFIS	**7,000,000**	**1,960,000**
	• Development	7,000,000	
	• Hardware		
	• Maintenance		1,400,000
	• Support		560,000
	Development of the ECRIS TCN system reference Implementation	**970,000**	**194,000**
	• Development	970,000	
	• Maintenance		194,000
	Update the ECRIS reference implementation	**259,200**	
	• Development	259,200	
	Technical specification for an ECRIS TCN system	**188,000**	

Scenario	Cost element	One-off *(in EUR)*	Recurring *(in EUR)*
	• Development	188,000	
	Update of the ECRIS technical specifications	**88,200**	
	• Development	88,200	
	Training personnel to collect fingerprints and search ECRIS using fingerprints		**110,685**
	• Training		110,685
Scenario 2B	**Total Scenario 2B**	**21,966,100**	**2,262,085**
	Upgrade National AFIS	**13,481,700**	
	• Development	9,510,000	
	• Hardware		
	• Software	3,971,700	
	Set up the ECRIS TCN system for distributed hit/no hit search queries in national AFIS	**7,000,000**	**1,960,000**
	• Development	7,000,000	
	• Hardware		
	• Maintenance		1,400,000
	• Support		560,000
	Development of the ECRIS TCN system reference Implementation for distributed queries	**957,000**	
	• Development	957,000	
	Update the ECRIS reference implementation	**259,200**	
	• Development	259,200	
	Technical specification for an ECRIS TCN system	**180,000**	
	• Development	180,000	
	Update of the ECRIS technical specifications	**88,200**	
	• Development	88,200	
	Maintenance of the ECRIS TCN system reference implementation		**191,400**
	• Maintenance		191,400
	Training personnel to collect fingerprints and search ECRIS using fingerprints		**110,685**
	• Training		110,685
Scenario 3A	**Total Scenario 3A**	**6,914,400**	**2,015,206**
	Set up the ECRIS TCN system at national level for querying a Central AFIS	**3,500,000**	**1,260,000**
	• Development	3,500,000	
	• Maintenance		700,000
	• Support		560,000
	Set up of Central AFIS system	**1,950,000**	**458,321**
	• Development	750,000	
	• Hardware	1,200,000	240,000
	• Maintenance		138,071
	• Support		80,250
	Development of the ECRIS TCN system reference Implementation	**931,000**	**186,200**
	• Development	931,000	
	• Maintenance		186,200
	Update the ECRIS reference implementation	**259,200**	
	• Development	259,200	

Scenario	Cost element	One-off *(in EUR)*	Recurring *(in EUR)*
	Technical specification for an ECRIS TCN system	**186,000**	
	• Development	186,000	
	Update of the ECRIS technical specifications	**88,200**	
	• Development	88,200	
	Training on the use of the fingerprints functionalities of ECRIS TCN system		**110,685**
	• Training		110,685
Scenario 3B	**Total Scenario 3B**	**15,902,200**	**2,015,206**
	Upgrade National AFIS for verification following a query in the central AFIS	**8,987,800**	
	• Development	6,340,000	
	• Hardware		
	• Software	2,647,800	
	Set up the ECRIS TCN system at national level for querying a Central AFIS	**3,500,000**	**1,260,000**
	• Development	3,500,000	
	• Maintenance		700,000
	• Support		560,000
	Set up of Central AFIS system	**1,950,000**	**458,321**
	• Development	750,000	
	• Hardware	1,200,000	240,000
	• Maintenance		138,071
	• Support		80,250
	Development of the ECRIS TCN system reference Implementation	**931,000**	**186,200**
	• Development	931,000	
	• Maintenance		186,200
	Update the ECRIS reference implementation	**259,200**	
	• Development	259,200	
	Technical specification for an ECRIS TCN system	**186,000**	
	• Development	186,000	
	Update of the ECRIS technical specifications	**88,200**	
	• Development	88,200	
	Training on the use of the fingerprints functionalities of ECRIS TCN system		**110,685**
	• Training		110,685
Scenario 4A	**Total Scenario 4A**	**6,914,400**	**2,015,206**
	Set up the ECRIS TCN system at national level for querying a Central AFIS	**3,500,000**	**1,260,000**
	• Development	3,500,000	
	• Maintenance		700,000
	• Support		560,000
	Set up of Central AFIS system	**1,950,000**	**458,321**
	• Development	750,000	
	• Hardware	1,200,000	240,000
	• Maintenance		138,071
	• Support		80,250
	Development of the ECRIS TCN system reference Implementation	**931,000**	**186,200**

Scenario	Cost element	One-off *(in EUR)*	Recurring *(in EUR)*
	• Development	931,000	
	• Maintenance		186,200
	Update the ECRIS reference implementation	**259,200**	
	• Development	259,200	
	Technical specification for an ECRIS TCN system	**186,000**	
	• Development	186,000	
	Update of the ECRIS technical specifications	**88,200**	
	• Development	88,200	
	Training on the use of the fingerprints functionalities of ECRIS TCN system		**110,685**
	• Training		110,685
Scenario 4B	**Total Scenario 4B**	**15,902,200**	**2,015,206**
	Upgrade National AFIS for verification following a query in the central AFIS	**8,987,800**	
	• Development	6,340,000	
	• Hardware		
	• Software	2,647,800	
	Set up the ECRIS TCN system at national level for querying a Central AFIS	**3,500,000**	**1,260,000**
	• Development	3,500,000	
	• Maintenance		700,000
	• Support		560,000
	Set up of Central AFIS system	**1,950,000**	**458,321**
	• Development	750,000	
	• Hardware	1,200,000	240,000
	• Maintenance		138,071
	• Support		80,250
	Development of the ECRIS TCN system reference Implementation	**931,000**	**186,200**
	• Development	931,000	
	• Maintenance		186,200
	Update the ECRIS reference implementation	**259,200**	
	• Development	259,200	
	Technical specification for an ECRIS TCN system	**186,000**	
	• Development	186,000	
	Update the ECRIS technical specifications		
	• Development	88,200	
	Training on the use of the fingerprints functionalities of ECRIS TCN system		**110,685**
	• Training		110,685

Source: KURT SALMON Data Analysis, April 2016.