European Commission

JRC SCIENCE FOR POLICY REPORT

Study on Fingermark and Palmmark Identification Technologies for their Implementation in the Schengen Information System

Administrative Arrangement JRC-34751

Haraksim, R
Galbally, J
Beslay, L

2019

Joint Research Centre

EUR 29755 EN

This publication is a Science for Policy report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

Contact information
Name: Laurent Beslay
Address: Joint Research Centre, Via Enrico Fermi 2749, 21027 Ispra, Italy
E-mail: laurent.beslay@ec.europa.eu
Tel.: +39 0332 78 5998

EU Science Hub
https://ec.europa.eu/jrc

JRC116442

EUR 29755 EN

PDF ISBN 978-92-76-03975-4 ISSN 1831-9424 doi:10.2760/852462

Luxembourg: Publications Office of the European Union, 2019

Figure 1 – source https://www.fbi.gov/news/stories/30-year-old-murder-solved and [52]
Figure 4 – source Carreira, L., Correia, P.L., Soares, L.D., *On high resolution palmprint matching*, Int. Workshop Biometrics Forensics, Valletta, Malta, March 2014, pp. 1-6 and https://www.fbi.gov/file-repository/guidelines-for-capturing-palm-prints-and-supplementals.pdf/view
Figure 5 – source [10]
Figure 6 – source https://www.fbibiospecs.cjis.gov/Latent/PrintServices

How to cite this report: Haraksim R., Galbally J., Beslay L., *Study on Fingermark and Palmmark Identification Technologies for their Implementation in the Schengen Information System*. EUR 29755 EN, Publication office of the European Union, Luxembourg, 2019, ISBN 978-92-76-03975-4, doi:10.2760/852462, JRC116442.

Table of contents

Abstract

The report assesses the technology readiness and availability of new functionalities – based on automatic fingermark and palmmark recognition technologies – for their integration into the Schengen Information System (SIS). These functionalities have been introduced in the revised SIS Regulations adopted on 28th of November 2018, both in the context of police and judicial cooperation.

The report is structured in two parts. In Part I, the automatic fingermark and palmmark recognition functionalities are introduced together with a review of the latest developments and state of the art, quality metrics and important biometric standards are provided; and it is concluded with a summary section entitled "lessons learnt".
In Part II, the functionalities are placed into the context of Schengen Information System. Use-cases for border control and police and judiciary cooperation in criminal matters are presented, and a list of recommendations for the successful implementation of fingermark and palmmark processing technologies into the Schengen Information System are provided.

Acknowledgements

This report was carried out by members of the DG JRC team in charge of the "*Biometric Research Applied to Security in the Schengen Area* (BRASSA)" project, working at the Cyber and Digital Citizens' Security Unit of Directorate E – Space, Security and Migration, Joint Research Centre. The study would not have been possible without the help, dedication and active involvement of a number of people working in different institutions all over Europe and beyond.
With our apologies to all those people who actively contributed to the study but are not explicitly mentioned hereafter, the authors would like to give a special recognition to:

DG HOME

We would like to thank the colleagues from the European Commission (EC) DG HOME Information Systems for Borders and Security Unit for their determinant support, comments and contribution, namely Messrs. Valerio Scandiuzzi, Philippe Van Triel, Richard Rinkens, Rob Rozenburg and Michael Flynn.

European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA)

We would like to thank all the colleagues from eu-LISA who provided us with insightful information and explanations on the operational management of some of the large-scale IT systems currently working in Europe, namely EURODAC, Visa Information System, and more specifically the Schengen Information System.

Representatives from EU Member States, Norway, Israel and United States of America Authorities

We would like to express our gratitude to the representatives of the six EU Member States visited and contacted during the fulfilment of the study: Estonia, France, Germany, Netherlands, Poland and Sweden.
We would like to thank the representatives of the associated EU Member State Norway, which also welcomed us during the development of the study.
We would like to express our gratitude to the colleagues from the Israeli Division for Identification and Forensic Sciences in Jerusalem.
We would like as well to thank the USA representatives from the National Institute for Standards and Technology (NIST), Department of Justice and the Federal Bureau of Investigation (FBI) for their great hospitality, openness and full cooperation.

Representatives from EU and international organisations

We would like to express our gratitude to the representatives of the EU and international organisations – FRONTEX and INTERPOL – who welcomed us during our study.

External experts review board

We would also like to thank the renowned international experts who joined the external scientific board of the study for reviewing its results and conclusions:

Prof. Christophe Champod, Université de Lausanne, Faculté de droit, des sciences criminelles et d'administration publique, Ecole des sciences criminelles, Lausanne (CH),

Ms. Melissa Gische, Forensic Expert, Federal Bureau of Investigation, Quantico VA (USA),

Didier Meuwly, Netherland Forensic Institute - The Hague, Special Chair in Forensic Biometrics - University of Twente (NL),

Prof. Daniel Ramos, Universidad Autonoma de Madrid, Escuela Politécnica Superior, Biometric Recognition Group – ATVS, Madrid (ES),

Dr. Elham Tabassi, National Institute of Standards and Technology, Washington DC (USA).

Executive summary

This report details the results of a DG JRC study on the readiness and availability of Automatic Biometric Identification System (ABIS) fingermark and palmmark[1] technologies for their introduction in the Central Schengen Information System (CS-SIS).

Policy context

Created as a compensatory measure for the abolition of internal border checks within the Schengen area, the SIS was established with two intentions: to contribute to police and law enforcement cooperation between the Member States and to support external border control. In its first generation the SIS was the first large-scale IT system launched by the EU Member States in 1995. It was followed by EURODAC (asylum seekers' database) in 2003 and the Visa Information System (VIS) in 2011. The second-generation of SIS entered into operation on 9 April 2013.

CS-SIS offers the possibility to process biometric data as it is already the case for EURODAC and the VIS. It was foreseen, according to Articles 22.c of CS-SIS Decision[2] and Regulation[3] from 2007, that CS-SIS could also be used to *identify* a person based on his/her *fingerprints*. This option required the implementation of an Automatic Fingerprint Identification System (AFIS) "*once it becomes technically possible*" and when the Commission had presented "*a report on the availability and readiness of the required technology on which the European Parliament is consulted*". In October 2015 DG JRC provided a report supporting the final decision of integrating 10-prints automatic fingerprint identification technology into the CS-SIS[4]. The CS-SIS AFIS went into production in March 2018.

Proposed in December 2016, a revision of the Regulation was approved on the 28th of November 2018, in the context of **police** and judicial cooperation[5], **border** checks[6] and the **return** of illegally staying third country nationals[7]. Extended functionalities which may be applied to the dactyloscopic data stored in the CS-SIS alerts are defined and in particular dactyloscopic data in SIS may also be searched using complete or incomplete sets of fingerprints or palm prints discovered at the scenes of serious crimes or terrorist offences under investigation.

In support of this newly adopted 2018 Regulation, the objective of the present DG JRC study is to determine whether fingermark and palmmark identification technologies are mature enough for their integration into the context of the SIS.

---

[1] The ensemble of fingermarks, palmmarks, fingerprints, palmprints, but also footprints (not considered in this report) is in forensic literature referred to as friction rige impressions.

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007D0533&from=EN

[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:381:0004:0004:EN:PDF

[4] https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/fingerprint-identification-technology-its-implementation-schengen-information-system-ii-sis

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1862&from=EN

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1861&qid=1544694006055&from=EN

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1860

The report presents the main findings of the study together with a series of recommendations for the successful implementation of ABIS fingermark and palmmark technologies in CS-SIS. The complete technical specifications of the ABIS systems to be integrated in the CS-SIS should be subjected to further study, ideally in the form of a benchmark test linked to the call-for-tenders issued to the vendors of the aforementioned technologies.

The JRC conducted an in-depth analysis of the fingermark and palmmark recognition technologies including a review of the scientific literature, visits to forensic laboratories in EU Member States and third countries, consultations with eu-LISA[8], FRONTEX and INTERPOL, and interviews of technology providers. An external scientific board of renowned international experts reviewed the results and conclusions of the study.

The report presents two main parts:

- **Part I** sets the scene on the current status of ABIS technology. It introduces the key parameters and concepts of ABIS systems, such as its feature extraction process, its matching algorithms, its performance evaluation, existing databases, quality of fingermark, fingerprint, palmmark and palmprint data or related standards.
- **Part II** introduces the SIS as it is implemented today, presenting some facts related to the current architecture and current use-cases as well as use-cases related to the fingermark and palmmark recognition technologies.

Key conclusions

Given the fact that large scale centralized IT systems are already successfully deployed at a national level for friction ridge modalities, the present study concludes that:

- ABIS-Fingermark systems have reached a sufficient level of readiness and availability for their integration into SIS, provided that the recommendations listed in the present report are implemented and respected, to the largest extent possible, during the rollout and utilization of the new functionality.
- ABIS-Palmmark systems have reached a sufficient level of readiness and availability for their integration into SIS, provided that the recommendations listed in the present report are implemented and respected, to the largest extent possible, during the rollout and utilization of the new functionality.

Main findings and Recommendations

The study identifies 21 recommendations to support the successful deployment and use of ABIS fingermark and palmmark functionalities in CS-SIS. The recommendations are mainly concerned with existing national expertise and best practice, selection of appropriate formats to collect, exchange and process data, production of statistics, identification of appropriate architecture options, application of rigorous procedures for biometric enrolment, selection of measures to foster quality, definition of use-case scenarios and introduction of regular performance evaluation actions.

[8] eu-LISA is the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

Related and future JRC work

In 2018, DG JRC conducted a study entitled "Automatic Fingerprint Recognition: From Children to Elderly Age and Ageing Effects[9]. This work was based on a dataset provided thanks to a collaboration with the Portuguese Authorities. The intention is to extend this study to account for the missing fingerprint data (i.e., fingerprints for adults aged 26-65 years old) and to confirm the trends reported.

In the absence of a robust, reliable and open-source fingermark, palmmark and palmprint image quality metrics, DG JRC has started to research the creation of such a quality metric. To this end, the JRC will need to acquire and, if not available, to produce, a ground-truth mated fingermark and palmmark datasets.

Quick guide

A Biometric Matching System (BMS) is a pattern recognition system used to search a biometric template, which is extracted from a friction ridge image (e.g. fingermark), in a database of biometric templates (e.g. fingerprints).

An ABIS is an Automated Biometric Identification System (contains a BMS) which implements a feature extraction and comparison algorithm. In particular, it extracts a biometric template from a submitted reference image and searches the reference biometric template database.

While the search using an ABIS-Fingerprint system produces a match / no-match response, the search using a ABIS-Fingermarks and Palmmarks system results in a rank-list of candidates, typically ordered by the magnitude of comparison score (high-to-low), which is evaluated by the fingerprint examiner who then makes a match / no-match decision.

[9] https://ec.europa.eu/jrc/en/publication/automatic-fingerprint-recognition-children-elderly-ageing-and-age-effects

List of recommendations

Recommendation 1:

Regular border crossing first line of check use-case 4P→TP use-case

In case ABC gates are used to process fingerprints of the travellers, we recommend implementation of liveliness detection to mitigate the possibility of a presentation attack.

If not the case yet, we recommend implementing automatic creation of CS-SIS compatible NIST containers for both border crossing scenarios (ABC gate and live-scan in front of the border guard), which is necessary for smooth interaction with the CS-SIS. If not the case yet, we recommend an automatic quality assessment to be implemented for both border crossing scenarios (ABC gate and live-scan in front of the border guard) to ensure, that only good quality fingerprints are consulted with the CS-SIS.

Given the strict time constraint at the first line of check, the border guard (or an ABC gate supervisor) should not be overwhelmed by an unnecessary amount of information. We recommend to make the feedback received from the CS-SIS as straightforward as possible, for example, no traveller-related information in CS-SIS (green light – traveller proceeds) and if information present in CS-SIS (amber light – traveller goes to the second line of check unless it is for discreet surveillance). We recommend that live-scan fingerprints are favoured over those stored in the passport.

Recommendation 2:

Dedicated search engines

We recommend maintaining a dedicated dataset of Unsolved Latent Files, which would be logically separated into fingermarks and palmmarks (if source is known) and marked source unknown otherwise.

We recommend to implement a dedicated search engine for fingermark → ten-print comparisons; ten-print → unsolved latent files comparisons; fingermark → unsolved latent files comparisons; palmmark → palmprint and palmprint → unsolved latent files comparisons.

Recommendation 3:

ABIS access to the CS-SIS ridge shape images

In order to take advantage of deep learning technologies, we recommend for the ABIS system to have access to targeted fingerprint and palmprint images stored in the CS-SIS, once the search-process on templates is completed and a rank list of candidates is produced (Face, Palmprint, ULF (Fingermark and Palmmark). The images of the palmprints / fingerprints of the rank-list of candidates, retrieved from the CS-SIS, would be used in a subsequent cascade search in which the images themselves would become the source of new texture features and thereby make the search results more accurate.

Recommendation 4:

Need for complementary statistics

Upon implementation of ABIS-fingermark and Palmmark search engine, we recommend following statistics be likewise collected from the Central System and National copies of the SIS: the number of consultations performed based on the ABIS-fingermark and Palmmarks; the number of person related alerts that contain fingermark images (Art. 40); the number of hits produced by the ABIS-fingermark search engine; the number of

duplicated alerts detected by the ABIS-fingermark search engine; the quality of the enrolled fingermark images in CS-SIS; the quality of the fingermark images submitted to perform consultations in CS-SIS.

Recommendation 5:

Benchmark test datasets built on SIS data

We recommend regular (every major update of the ABIS system used, but also periodically every 3-5 years) benchmark performance evaluations, after a first performance assessment of participating technology providers to be a part of the call-for-tender before selecting a new ABIS technology.

For this purpose, we recommend to develop and maintain, with the direct participation of the Member States (responsible of the data) a dedicated benchmark database with known ground truth for all kind of friction-ridge modalities based on the real data of SIS.

Recommendation 6:

Friction ridge image resolution

We recommend the fingermark and palmmark images to be stored in 1000dpi (or higher) resolution. As confirmed by the different vendors, the current COTS algorithms are capable of processing dactyloscopic traces in this resolution.

Note: In case when the reference database is recorded (and maintained) at 500dpi, the higher resolution fingermarks and palmmarks are simply down-sampled.

Recommendation 7:

Common interchange standard

We recommend adhering to the ISO 39794 biometric standard for exchange of minutiae and EFS, which will be sustainable in the long term. This standard accounts for future developments in the areas of feature extraction and comparison and ensures forward-backwards template compatibility.

Recommendation 8:

Parameters for evaluating accuracy of ABIS system

We recommend to clearly define a set of parameters that will be used in the evaluation of the overall performance of the ABIS-system.

Recommendation 9:

Fingermark image quality metrics

We recommend, when technology becomes available, the implementation of fingermark quality assessment (Fingermark Quality Metric) into the CS-SIS processing pipeline.

In cases strictly linked to the Art. 40 we recommend to allow the MSs to create alerts using fingermarks of "insufficient" image quality (e.g. ABIS not capable of producing a biometric-searchable template), as these may become "searchable" in the (near) future.

Recommendation 10:

ROI and number for fingermarks per SIS consultation

It has been suggested by some providers and users, that fingermark and palmmark feature extraction and comparison algorithms may perform more efficiently if one single fingermark is present in the image submitted. We recommend cropping the image

containing fingermark to the ROI, in cases when multiple fingermarks are present in the image.

Recommendation 11:

Quality check in absence of Quality Metric

In the absence of robust and reliable fingermark / palmmark image quality metric we recommend to:

- Identify and share best practices applicable to SIS between MS and maintain a common repository of these best practices.

- Use the National AFIS in an attempt to produce a NS-AFIS searchable template. Should a National AFIS be capable of producing a template, the ABIS-fingermark and palmmark implemented at the CS-SIS should "in principle" be capable as well of producing an ABIS-searchable template.

- Allow the MS to finalise the creation of an alert (art. 40) with a fingermark/palmmark which failed to produce an ABIS-searchable template. The alert will be flagged as not searchable but it is likely that forthcoming technology development will allow extraction of ABIS-searchable template from these images in the near future.

Recommendation 12:

Rank list size and feedback from the CS-SIS

Given that the operating parameters of the fingermark and palmmark ABIS are yet to be defined (or they will become known after a benchmark vendors evaluation is performed during the call-for-tender), we recommend to fix by default the number of returned candidates to 20 (which constitutes a conservative average observed during the visits at national laboratories). A possibility should be given to the consulting officer to request a longer rank list. We further recommend that the rank lists are completed with comparison scores.

Note: Once the performance parameters of the implemented technology are known, the rank lists could be converted into "dynamic". The size of such a rank list could be calculated for example as a function of distance of rank 1 score to the cohort of nearest 5 ranks.

Recommendation 13:

Use-case LP → TP

In case of a **No-Hit,** the consulting officer should re-label a fingermark as a palmmark, as the "alleged" fingermark may have originated from a palm and thus may produce a hit in the BMS-palmprint database. Alternatively, it could be possible to search immediately on both.

We recommend using a dedicated ABIS feature extraction algorithm, which is capable of extracting the fingermark-searchable templates from fingerprint images for creation of the alerts in the BMS-ULF.

Recommendation 14:

Use-case TP → LP

We recommend using a dedicated ABIS search algorithm that is capable of extracting the fingermark -searchable templates from ten-print fingerprints to consult BMS-ULF database.

Recommendation 15:

Use-case LP → LP

We recommend that the real-time Fingermark to ULF database search should be reserved for extreme cases of high threat of terrorism and/or serious criminal activity.

We recommend performing a batch comparison of unsolved fingermarks with the ULF database periodically, sort the candidates by the highest score and apply a pass threshold to reveal potential matches in the BMS-ULF database.

Recommendation 16:

Live-scan images in the 4P → LP use-case

Whenever possible, we recommend using live-scanned fingerprints instead of the fingerprints stored in the passport for CS-SIS consultation.

Recommendation 17:

Regular border crossing and high decision threshold for 4P → LP

From the operational point of view and given the two different applications – the law enforcement and the regular border crossing, we recommend using a "binary flag" to distinguish between the consultation originating at the border and at the police station. In case of border crossing, a high decision threshold should be applied when searching against the ULF, and the border guard should be informed of a pseudo-match only when an Art 40 alert is above this high decision threshold.

Recommendation 18:

Dual use fingermark and palmmark in LPP → PP use-case

We recommend encouraging the consulting officer to encode an initially declared fingermark as a palmmark in case of a **No-Hit**, as the supposed fingermark might have originated from a palm and thus may produce a hit in the BMS-palmprint database.

We recommend using a dedicated ABIS feature extraction algorithm that is capable of extracting the palmmark-searchable templates from palmprint images for creation of the alerts in the BMS-ULF. (***recs. 9, 10, 11*** and ***12*** apply).

Recommendation 19:

Use case PP→ LPP

We recommend using a dedicated ABIS search algorithm that is capable of extracting the palmmark-searchable templates from palmprint images for consulting the BMS-ULF database.

Recommendation 20:

Standardized Minutiae and EFS interchange format for the CS-SIS

We recommend adopting for the Central System of SIS a solution in compliance with a standard for Minutiae and EFS interchange format, such as the new ISO/IEC 39794-1 and ISO/IEC39794-4 when become available, as they guarantee forward and backward interoperability.

Recommendation 21:

Progressive implementation leading eventually to an EU-Universal Template Converter (EU-UTC)

We recommend in a first stage to allow a fully lights-out mode only (case A together with option A). This first step can be quickly achieved as soon as the future selected fingermark ABIS for the CS-SIS enters into production.

Then in a second step, in order to allow cases B, C and D and to increase accordingly the accuracy of the fingermark ABIS, an EU-UTC API (option E) (which would take as an input a friction ridge image accompanied by the information necessary for creation or consultation of an alert, and automatically produce CS-SIS compliant templates according to the needs/desires of the operator), should be developed and distributed to the MSs in order to be introduced a national level.

List of figures

List of tables

Main acronyms and abbreviations

ABIS	Automatic Biometric Identification System
AFIS	Automatic Fingerprint Identification System
BIF	Bayesian Interpretation Framework
CNN	Convolutional Neural Network
CS-SIS	Central System - Schengen Information System
DG	Directorate General
DHS	Department of Homeland Security
DIFS	Division of Identification and Forensic Sciences, Israel
EC	European Commission
ECRIS	European Criminal Records Information System
EES	Entry Exit System
ENFSI	European Network of Forensic Science Institutes
EU	European Union
FBI	Federal Bureau of Investigation
FPIR	False Positive Identification Rate
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
JRC	Joint Research Centre
LR	Likelihood Ratio
MS	Member State
NIST	National Institute for Standards and Technology
SIS	Schengen Information System
VIS	VISA Information System

Introduction

The Schengen Information System (SIS) is the most widely used and largest information sharing system for **security** (law-enforcement) and **border management** in the European Union. Throughout this report, it is important to bears in mind the two intertwined dimensions of SIS: law-enforcement and border management. While the system is unique, it has to deal with the reality of these two contexts which, in some cases, present different challenges and constraints. Just to give an example, at the first line of check, a border guard has very limited time to take a decision on a traveller, while in a police station an officer has almost no technical limitation time-wise to do the necessary checks on a subject. This dual use of SIS leads to differences in the use-cases of the system that will be highlighted in the report.

The main purpose of SIS is to make Europe safer. The system assists the competent authorities in Europe to preserve internal security in the absence of internal border checks. To reach this objective, SIS enables competent national authorities, such as the police and border guards, to enter and consult **alerts** on **persons** or **objects**. A SIS alert always consists of three parts:

- A set of data for identifying the person or object, subject of the alert,
- A statement why the person or object is sought after, and
- An instruction on the action to be taken when the person or object has been found.

The quality, accuracy and completeness of the data elements enabling identification are the key conditions for the success of SIS. For alerts related to persons, the minimum data set consists of name, year of birth, a reference to the decision giving rise to the alert and the action to be taken. When available, facial images and fingerprints must be added to facilitate identification and to avoid misidentification.

SIS consists of three major components:

- A Central System, CS-SIS,
- The national systems, N-SIS,
- A communication infrastructure (network) between the systems.

An alert entered in SIS in one MS is transferred in real-time to the central system. It then becomes available in all the other MSs so that authorized users can search the alert on the basis of the entered data-elements. Specialised national SIRENE bureaus located in each MS serve as single points of contact for the exchange of supplementary information and coordination of activities related to SIS alerts. The responsibility of SIS management is divided as follows:

- Each **MS** using the CS-SIS is responsible for setting up, operating and maintaining its national system and its national SIRENE bureau.
- The EU Agency for large-scale IT systems (**eu-LISA**) is responsible for the operational management of the central system and the communication infrastructure.
- The **EC** is responsible for the general supervision and evaluation of the system and for the adoption of implementing measures where uniform conditions for implementation are needed, such as the rules for entering and searching data.

Towards the end of 2018[10], SIS contained approximately 82.2 million records (i.e., alerts), out of which, 940K were related to persons and the rest to objects. From the person alerts, around 25% contained at least one fingerprint image and around 30% contained at least one facial image.

In 2018, SIS processed a total of 6.2 billion queries (including queries related to both object and person alerts), out of which around 0.005% were processed by the current AFIS.

For further details on the current functionality of CS-SIS we refer the reader to PART II of the present study.

I. Policy, technical and legal context of CS-SIS

The second-generation Schengen Information System entered into operation on 9 April 2013. SIS has been the first so-called large-scale IT system launched by the EU MSs in 1995 and has been followed later by EURODAC (asylum seekers database) in 2003 and the Visa Information System (VIS) in 2011.

Note: A predecessor of the centralised large-scale IT systems such as CS-SIS, CS-VIS, CS-ECRIS is the Prüm system, developed by the EU Member States under the umbrella of the Prüm Treaty[11] and later in the context of the Decision 2008/615/JHA[12], which allowed "peer-to-peer" process of biometric data (including DNA), vehicle registration data and query national criminal databases. It is used to foster the police cooperation amongst 27 EU member states. A brief comparison between the Prüm system and CS-SIS is presented in a comparison table in Annex 1: Comparison table of Prüm and CS-SIS. The Prüm system is not part of the study, but it has been highlighted and discussed with the Member States visited and deserves to be mentioned.

From the operational point of view, the CS-SIS and Prüm present two different approaches. While in Prüm, a connection is established between the MS submitting a query and one or several MS receiving it, which launches an AFIS search on their own ***National System*** (the consultations are treated by the ***MS receiving*** the request), the SIS is a centralized system which contains an AFIS system and a reference 10-print cards database populated by the MS built in. The central system of the SIS, the CS-SIS AFIS performs the comparison on the consulted fingerprint 10-print card and returns a match / no-match response, accompanied by a comparison score, to the consulting MS.

CS-SIS offers the possibility to process biometric data as it is already the case for EURODAC and the VIS. It was foreseen according to Articles 22.c of CS-SIS Decision[13] and Regulation[14] from 2007 that CS-SIS could also be used to *identify* a person on the basis of his/her *fingerprints*. This option required the implementation of an Automatic Fingerprint Identification System (AFIS) "*once it becomes technically possible*" and when the Commission had presented "*a report on the availability and readiness of the required technology on which the European Parliament is consulted*". In October 2015 DG JRC

[10] https://www.eulisa.europa.eu/Publications/Reports/SIS%202018%20statistics.pdf

[11] http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010900%202005%20INIT

[12] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008D0615&from=EN

[13] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007D0533&from=EN

[14] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:381:0004:0004:EN:PDF

provided such a report supporting the final decision of integrating 10-prints fingerprint identification technology within the functionalities of CS-SIS[15]. The CS-SIS AFIS went into production in March 2018.

In December 2016, following the decision to integrate 10-print fingerprint identification technology in CS-SIS, a revision of the Regulation was proposed which was finally approved on the 28th of November 2018, for police and judicial cooperation[16], border checks[17] and and for the return of illegally staying third country nationals[18]. In article 33 of the new SIS-Border checks regulation and article 43 of the new SIS-Police and judiciary cooperation regulation, it is defined the new use that can be given to dactyloscopic data stored in alerts:

- Article 33.2 Border checks and Articles 43.2 Police cooperation:

  "Dactyloscopic data may be searched in all cases to identify a person. However, dactyloscopic data shall be searched to identify a person where the identity of the person cannot be ascertained by other means. For that purpose, the Central SIS shall contain an Automated Fingerprint Identification System (AFIS)."

- Article 33.3 Border checks and Article 43.3 Police cooperation:

  "Dactyloscopic data in SIS in relation to alerts entered in accordance with {Articles 24 and 25 for border, Articles 26, 32, 36 and 40 for police} may also be searched using complete or incomplete sets of fingerprints or palm prints discovered at the scenes of serious crimes or terrorist offences under investigation, where it can be established to a high degree of probability that those sets of prints belong to a perpetrator of the offence and provided that the search is carried out simultaneously in the MSs relevant national fingerprints databases."

In support of the 2018 Regulation, the objective of the present study is to determine the readiness of fingermarks and palmmark recognition technologies, to be integrated in CS-SIS for the identification of a person.
While the main focus of the 2015 JRC study was on the readiness and availability of fingerprint recognition technology for comparing friction ridge impressions in a form of fingerprint 10-print cards, the present study focuses on fingermarks and palmmarks recognition. The difference is illustrated in **Figure 1**, which depicts the three dactyloscopic modalities – a fingermark and a good quality fingerprint as reported by FBI[19], and a high resolution palmprint record from a THUPALMLAB database.

Fingermarks can in principle be searched by an AFIS-system, provided that templates containing fingerprint features vectors of the 10-print fingerprints have been produced in a "*fingermark-searchable*" way (not the case yet in the present-day CS-SIS AFIS).

---

[15] https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/fingerprint-identification-technology-its-implementation-schengen-information-system-ii-sis

[16] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1862&from=EN

[17] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1861&qid=1544694006055&from=EN

[18] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1860

[19] https://www.fbi.gov/news/stories/30-year-old-murder-solved

However, the level of accuracy of such AFIS system when searching fingermarks will be lower compared to searches on good quality 10-print fingerprints.

Full palmprints, partial palmprints and palmmarks cover much larger surface area, therefore it is common to use different automatic recognition algorithms, although, some vendors integrate the palmprint matching capabilities in their fingerprint recognition solutions.

Figure 1. Example of high-resolution fingerprint, fingermarks and high resolution palmprint record (murder case solved by FBI, right example from the THUPALMLAB DB. (Source: FBI)

Note: The terms *fingermark* and *palmmark* used in this report refer to fingerprints and palmprints found on crime scenes, which are usually partial, as they result from imperfect impositions of actual fingerprints/palmprints. They are very often in latent form meaning that they need to be visualized using methods and tools developed for the purpose of forensic investigation. Unlike the "latents", fingermarks and palmmarks referred to in this report are visible to a human eye and for the sake of simplicity assumed to be available in a form of digital images.

As explained above, although sufficient difference exists between "fingermarks" and "latent prints" (idem for "palmmarks" and "latent palmprints"), in many documents the terms are used as synonyms. Generally speaking, the literature published in the USA commonly refers to "latent prints / palmprints" while in Europe a preferred term is "fingermarks" / "palmmarks".

II. Objectives of the study

In support of the new 2018 Regulation presented in Section I, the objectives of the present DG JRC study are to:

OBJECTIVE 1: Determine the readiness of fingermark and palmmark recognition technologies, to be integrated into CS-SIS for the identification of a person.

OBJECTIVE 2: Provide recommendations on the best way to integrate fingermark and palmmark recognition technologies in CS-SIS based on:
1) the current state of the art of these technologies;
2) the particularities and constraints of CS-SIS and its dual use for law-enforcement and border management.

As will be further explained in Section V, to reach these two objectives, the present report describes first in PART I the current state of the art in ABIS-Fingermark and ABIS-palmmark recognition technology and states the challenges faced by this type of systems. Then, in PART II, it contextualises the technology given the specificities of CS-SIS, offering a series of recommendations on how to best address these challenges for the successful outcome of the eventual integration of new ABIS technology in CS-SIS.

III. Technology: Readiness and Availability

According to the Horizon 2020 EU Research and Innovation Framework Program, the readiness and availability of a given technology is assessed using the following nine Technology Readiness Levels (TRL):

- TRL 1 – basic principles observed,
- TRL 2 – technology concept formulated,
- TRL 3 – experimental proof of concept,
- TRL 4 – technology validated in laboratory,
- TRL 5 – technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies),
- TRL 6 – technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies),
- TRL 7 – system prototype demonstration in operational environment,
- TRL 8 – system complete and qualified,
- TRL 9 – actual system proven in operational environment.

As will be explained in this report, although AFIS technology has reached TRL 9[20], with multiple large-scale systems already deployed and working worldwide, each operational scenario has its own specificities. As such, the successful application of a certain

[20] Similar classification and approach can also be found in the report "Best Practices in Testing and Reporting Performance of Biometric Devices" by Wayman and Mansfield from 2002. http://www.kisa.or.kr/jsp/common/downloadAction.jsp?bno=59&dno=9&fseq=1

technology to a given specific use-case and environment, does not necessarily guarantee the same level of success when those operational conditions are changed.

In particular, for AFIS technology to achieve the expected level of performance, there are certain parameters that have to be considered. Probably, the most important of these features is the **accuracy** that can be expected from an ABIS-Fingermark, ABIS-Palmmark or ABIS-palmprint system. Unfortunately, the answer to the question of how accurate current systems are is not straightforward, as it largely depends on the data (i.e. fingerprint and fingermark samples) a system will have to deal with and, more particularly, with the **quality** of that data. Furthermore, depending on the **use-cases** defined for a given ABIS-Fingermark, ABIS-Palmmark or ABIS-palmprint system, a different level of accuracy may be acceptable and/or expected for different operational conditions/scenarios.

This report describes current ABIS-Fingermark, Palmmark and Palmprint technologies and states the challenges faced by these types of systems.

IV. Methodology followed

The study was conducted in three steps with some slight overlap between them:

- Step 1: Wide collection of information regarding ABIS-Fingermark, Palmmark and Palmprint technologies.
- Step 2: Synthesis of the information obtained from multiple sources.
- Step 3: Production of the report.

Step 1 was the most important and, as such, the most time and resource consuming. This step provided all the necessary information for the analysis and eventually led to the current report. This information was collected over five phases, each of them involving different sources. These phases are detailed in the next sections.

Phase 1: Analysis of the state of the art in ABIS-Fingermark, Palmmark and Palmprint technology

Relevant bibliography and scientific literature were extensively reviewed in order to consolidate and complement existing JRC knowledge and obtain an initial solid overview of the main features and challenges of ABIS-Fingermark, Palmmark and Palmprint systems. This scientific review contributed to the preparation of a set of visits and consultations carried out in the subsequent phases and complemented the information collected during those visits.

Phase 2: Consultation with national ABIS-Fingermark and Palmmark operators

The end-users of a future ABIS technologies in CS-SIS will be the competent authorities of the different MSs such as law-enforcement and border-control authorities. It is therefore extremely important to appreciate the operational contexts in which MSs are using their national ABIS-Fingermark, Palmmark and Palmprint systems, the similarities and differences between them, as well as to understand their operational needs.

Following the rationale described above and in order to address the objective of assessing "*the availability and readiness of the required technology*" for the inclusion of an ABIS-Fingermark and Palmmark systems in CS-SIS, the JRC first contacted and visited six EU Schengen MSs' law-enforcement and border-control entities (Germany, Netherlands,

France, Poland, Sweden and Estonia) and the law-enforcement agency and border control entity of Norway. The choice of the MS participating to this study was based on the availability and operational status both – ABIS-Face and ABIS-Fingermark/ABIS-Palmmark technologies. The preference was also given to the MSs with experience/operation of both ABIS systems or/and which were not visited during the JRC 2015 study. The objectives of these visits were threefold:

- Obtain knowledge regarding the technical aspects of the ABIS-Fingermark and Palmmark solution implemented in these countries,
- Identify the operational constraints and best-practice followed,
- Describe the challenges faced.

The visits to MS have led to better understanding and subsequently to a definition of the use-casers, in which the MSs were using their national ABIS-Fingermark, Palmmark and Palmprint systems, national AFIS, as well as their access to CS-SIS AFIS or any other AFIS (e.g. EURODAC, VIS, Prüm, Interpol). The visits gave also the opportunity to collect the possible expectations and recommendations these authorities might have regarding the introduction of ABIS-Fingermark and Palmmark functionalities in CS-SIS.

The visits to the seven Schengen Countries were complemented with a visit to the United States of America (US), the host of some of the biggest and most advanced ABIS-Fingermark, Palmmark and Palmprint systems, presenting broad similarities with the objectives and expected use of the CS-SIS ABIS-Fingermark and Palmmark technologies. It was followed by the visit to Israel which presents a very rich operational experience in using ABIS-Fingermark, Palmmark systems.

In addition to the visit to Eu-LISA (see next section), two EU and international organizations – Frontex and Interpol, both having operational experience with the use of this technology were also visited.

These visits were facilitated by the permanent support of DG HOME colleagues during the SISVIS committee meetings during 2018. Prior to each visit, an outline of the envisaged technical exchanges was sent to the selected countries (see

Annex 2: Outline of Technical meeting with MSs national experts for fingermark recognition discussion). This outline aimed to inform them by providing a list of preliminary questions regarding the different technical fields the JRC wished to explore during the visit. Each visit focused on the following subjects:

- Identification of the use-cases in which fingermarks, palmmarks and palmprints are processed,
- A technical description of the national ABIS-Fingermark, Palmmark and Palmprint system,
- The management of the life cycle of fingermarks and palmmarks in their system,
- The possibility to have a live demonstration of the use of the relevant ABIS systems.

The JRC visits were focused on national ABIS systems used in the context of criminal-investigation and managed by national police forces. However, for each visit, authorities in charge of border-control (having access to the national ABIS-Fingermark, Palmmark and Palmprints) were invited to participate in the presentations and discussion. At the beginning of each visit, the JRC gave an introductory presentation and proposed an agenda divided into four main steps:

- The National AFIS;
- The National ABIS-Fingermark, Palmmark and Palmprint system;
- Current and future uses of CS-SIS;
- Use of other EU/international system such as Prüm, INTERPOL, etc.

The visits were conducted by two JRC scientific officers. A team of two was necessary to cope with the rich and intensive discussion offered by the visited countries. At the end of each visit, the JRC provided the timescale of the study and invited participants to review the final draft of the present report. The timeline and most relevant information concerning the visits are summarized in **Table 1**.

Table 1. Summary of the key information concerning the visits to the institutions managing the national AFIS in different countries

VISIT	DATE	INSTITUTION
eu-LISA	05/02/2018	Strasbourg, France
Norway	01/03/2018	National Criminal Investigation Service (Oslo)
The Netherlands	06/03/2018	National Police Corps (Zoetemeer)
Germany	11/03/2018	Federal Criminal Police Office -BKA (Wiesbaden)
USA	26/03/2018	US National Institute for Standards and Technology (NIST) Federal Bureau of Investigation (FBI) – Criminal Justice Information Services (CJIS) Federal Bureau of Investigation (FBI) – Criminal Justice Information Services (CJIS) – Latent Print Support Unit
Israel	16/04/2018	Department of Identification and Forensic Science - DIFS (Jerusalem)
France	20/04/2018	Institut de Recherche Criminelle de la Gendarmerie Nationale - IRCGN (Paris)
Poland	25/04/2018	National Police Forensic Service (Warsaw)
FRONTEX	26/04/2018	FRONTEX (Warsaw)
Sweden	10/09/2018	National Forensic Centre - NFC (Linköping)
INTERPOL	26/09/2018	Lyon, France
Estonia	15/11/2018	Intelligence Management and Investigation Department (Tallinn)

Phase 3: Consultation with eu-LISA

The visit to the European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) provided an accurate picture of the CS-SIS AFIS currently in operation, EURODAC and the Visa Information System (VIS) as well as considerations regarding EU AFIS systems forthcoming such as, European Criminal Records Identification System (ECRIS) and the EU Entry Exit System (EES). It also provided a detailed description of the CS-SIS central system and its reporting capability. This visit was followed by a series of exchanges and conference calls with the officers respectively in charge of CS-SIS, VIS and EURODAC until the end of the study, providing the latest up-to-date statistics of those systems when available.

Phase 4: Consultation with ABIS technology vendors

The information collected from authorities already using ABIS-Fingermark was completed by discussions with some of the main providers of such a technology. This allowed the JRC to have a better understanding of the deployment challenges faced by the actual designers of such systems. Although numerous companies offer ABIS-fingermark in multiple domains, most of them are integrators and do not themselves develop AFIS solutions as it is the case with the ones contacted (Idemia, Gemalto and NEC).

Phase 5: Review by the external board

The previous information sources (i.e., review of the state-of-the-art, visits to international organizations and consultation at the premises with the eu-LISA) constituted the main foundation of the study and allowed JRC to draft the report on the integration of fingermark and palmmark recognition technologies in SIS. This process led to the production of a number of conclusions and recommendations extracted from the information gathered.

In order to review the results and conclusions established in this report, an External Review Board was established. This expert review board was composed of five internationally renowned researchers and experts in the concerning field. Their main objective was to review the report in order to 1) give comments that can complement/improve its quality, 2) correct possible content mistakes and 3) suggest missing pieces of relevant information. The final draft version of the report was submitted to the members of the external review board at the end of December 2018. The five experts presented their reviews, comments and suggestions in the course of meetings between the end of January 2019 and mid-February 2019.

V. Structure of the report

The approach adopted by the JRC for the initial analysis had as main objective to explore and assess the main characteristics and challenges of ABIS Fingermark and Palmmark technologies from a general perspective and then apply these identified elements to the specific context of SIS and suggest recommendations to appropriately address them. Accordingly, the JRC report contains two main parts:

- **PART I** sets the scene on the current status of ABIS Fingermark and Palmmark technologies. It introduces the key parameters and concepts of ABIS Fingermark and Palmmark systems, such as its feature extraction process, its matching algorithms, its performance evaluation, existing databases, quality of fingermark and palmmark data or related standards.

  The last section is dedicated to the main challenges faced by ABIS Fingermarks and Palmmarks developers when implementing these systems. All the challenges have been extracted from the large amount of information provided by the different sources consulted during the preparatory stages of the report (i.e. bibliography, MSs, vendors, eu-LISA, and external experts board).

- **PART II** introduces the SIS as implemented today, presenting some facts related to the current architecture and current use-cases.

  Following the initial presentation of the current system, and supported by concepts and key features for the ABIS Fingermark and Palmmark technology detailed in PART I, PART II presents those functionalities in the light of the specificities of SIS. These result in a series of recommendations, suggestions and options on how each of the challenges presented at the end of PART I could be potentially dealt with in the use-cases identified for SIS in order to successfully implement an ABIS Fingermark and Palmmark functionality in the most effective way possible.

  This part finishes with a more prospective look into the future giving some possible actions (not contemplated by the current legislation) that could be envisaged in

the years to come in order to further improve the accuracy, effectivity and ultimately the added-value offered by SIS to the MSs.

VI. Audience of the report

Even though some general aspects of SIS are presented in the introduction of the report, the document has been thought for readers with knowledge of SIS and basic understanding of biometric technology. The reader should bear in mind that many details about the functioning and purpose of SIS are not described here as they are assumed to be known.

Regarding the biometric dimension, although the report has been conceived as a self-contained document to be read by a wide audience, many specific aspects related to biometric technology are discussed in the different sections (especially in PART I). Therefore, for those readers who are laymen in biometrics, it is strongly recommended to first read some general introduction to biometrics such as the research overview articles [1] [2], or the standardised biometric tutorial "ISO/IEC TR 24741 Biometrics – Overview and Application". In these documents basic concepts related to biometric technology are described. This initial reading can contribute to a better grasp of the implications and findings of the report.

VII. A note on terminology

The present document tries to adhere, to the largest extent possible, to the standardised biometric vocabulary that can be consulted in the international standard[21] "ISO/IEC 2382-37 – Information Technology – Vocabulary – Part 37: Biometrics".

The reader should be aware that the definitions given in the SIS Regulation and the standardised vocabulary may not be exactly equivalent. In these cases, priority has been given to the definitions provided by the Regulation. As such, unless specified otherwise, the next definitions taken from Article 3 of the Regulation are used:

[21] Freely available at: http://standards.iso.org/ittf/PubliclyAvailableStandards/c066693_ISO_IEC_2382-37_2017.zip

Match. A match means the occurrence of the following steps:

- a search has been conducted in SIS by an end-user,
- that search has revealed an alert entered into SIS by another MS, and
- data concerning the alert in SIS match the search data.

Hit. A hit means any match which fulfils the following criteria:

- it has been confirmed by the end-user or by the competent authority in accordance with national procedures, where the match concerned was based on the comparison of biometric data, and further actions are requested.

Biometric data means personal data resulting from specific technical processing relating to the physical or physiological characteristics of a human being, which allow or confirm the unique identification of that human being, particularly photographs, facial images, dactyloscopic data and DNA profile.

Dactyloscopic data means data on fingerprints and palmprints which due to their unique character and the reference points contained therein, enable accurate and conclusive comparisons on a person's identity.

Fingermark and **Palmmark**, means a digital impression of a partial fingerprint/palmprint, typically recovered in a course of a crime scene investigation.

Part I
Overview of ABIS Fingermark and Palmmark technology

Automatic Fingerprint Recognition Systems (AFIS) have been around for nearly half a century with one of the first AFIS systems put in operation in 1974 by the FBI. This system, unlike the AFIS systems of today, only stored fingerprint minutiae configurations, but still helped to drastically cut down the fingerprint processing times from several days to 100,000 fingerprint sets in half an hour. Soon after, private companies realised a potential of AFIS solutions and entered the market. Morpho (currently IDEMIA) was amongst the very first (formed around 1982).

Over the last few decades we witnessed increase in computing power, development of more reliable computer architecture and tremendous increase in storage capacity, which all helped to integrate and process fingerprints on much larger scale. The technological advances went hand in hand with the development of fingerprint feature extraction and matching algorithms, which nowadays are faster, more accurate and more reliable than ever before. The world-wide adoption, popularity and use of AFIS systems, in particular in law enforcement, comes therefore as no surprise.

The break of the millennia witnessed development of integrated AFIS solutions supporting both – finger and palm print searches, following the rationale that a significant portion of the dactyloscopic trace evidence recovered from the crime scenes could be attributed to the palmprints. The report published by the NSTC (USA) derived from the operational experiences of law enforcement agencies suggested this number to be around 30%. Since then, palmprint recognition systems became widely adopted by the law enforcement agencies and palmprints are searched on the regular basis when crime-scene traces are consulted.

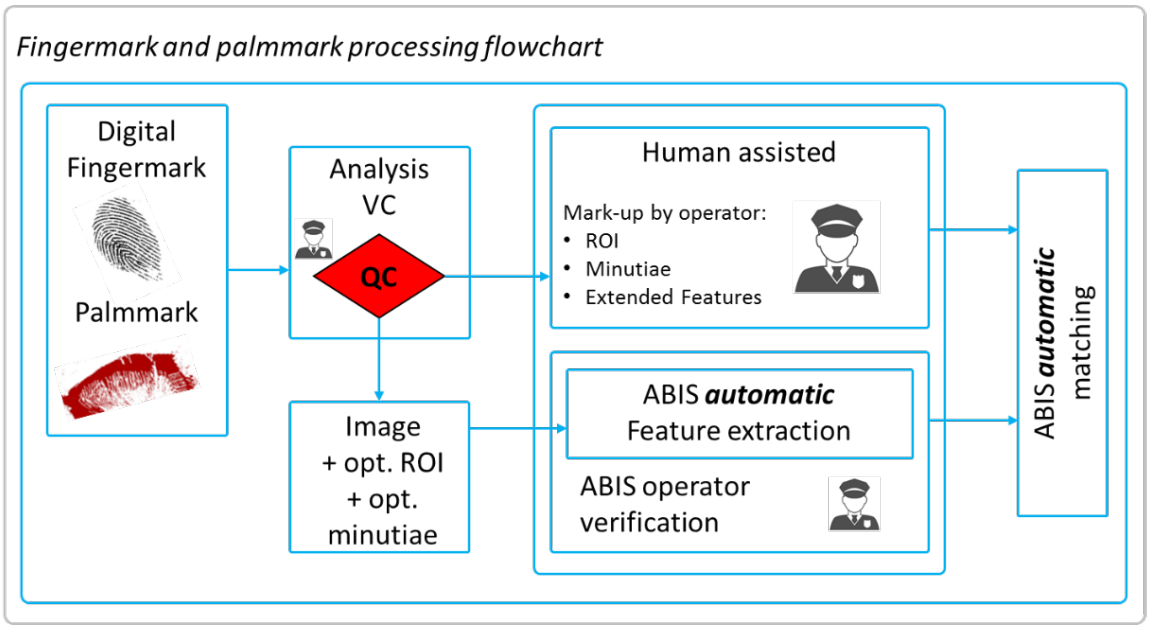
Nowadays, the integrated AFIS solutions are slowly being replaced by Automated Biometric Identification systems, which in addition to automatic fingerprint / fingermark / palmprint recognition support also the automatic face and iris recognition (potentially other biometric modalities).

This part of the report introduces the fingermark and palmmark recognition technology, presents the latest developments as a review of the state of the art, describes biometric sample quality, international standards. It is concluded by a summary of challenges, faced when developing and integrating an automated fingermark / palmmark recognition system.

1. Overview of ABIS-Fingermark technology

Fingermarks are closely linked to the forensic Crime-Scene (CS) investigation. The "life" of a fingermark begins as a partial impression left by an unknown suspect, often on a surface of an object manipulated, be it glass, plastic, metal, wood, paper, paint, blood etc. As will be shown later in the summary of best practices across the MSs (MS) visited, the fingermarks are collected from the CS by trained members of the police force. Depending on the type of material, different techniques are used by the CS investigators and laboratory technicians to develop the fingermark. Discussion regarding fingermark visualization techniques are beyond the scope of this study, though interested readers are welcome to review for example the UK's Home Office Fingerprint Sourcebook[22] or the ENFSI Best Practice Manual for Fingerprint Examination[23]. The resulting product of the fingermark development process is the fingermark[24], a "visible-to-human-eye" digitized partial impression, which is subjected to further analysis performed by the forensic laboratories.

Figure 2. Processing crime-scene recovered marks (Source: EC 2018)



Given the nature of this exercise – the crime-investigation – the desired outcome of the fingermark evaluation is the individualization, a link between the fingermark recovered from the crime scene and one of the fingers of the perpetrator – the person whose finger has left the fingermark. The individualization protocol followed by vast majority of the fingerprint laboratories is called ACE-V procedure [3], consisting of 4 steps:

[22] https://www.gov.uk/government/publications/fingerprint-source-book-v2

[23] http://enfsi.eu/wp-content/uploads/2016/09/6._fingerprint_examination_0.pdf

[24] **Fingermark** is preferred term in continental Europe, while in the USA and Canada the preferred term is "**latent**" fingerprint. Given the target audience of this study the term **fingermark** will be used throughout this study.

- **Analysis** – determination of "value" of fingermarks using adequate (visual) assisting tools. Three levels are traditionally used to determine the value of fingermarks – Value for Comparison (VC) or No Value (NV), out of which the VC fingermarks make it to the comparison phase. The result of this process is a feature vector (or an extended feature vector) containing position and orientation of minutiae, singularity points and/or additional features which will be used in the next step. A simplified workflow is depicted in **Figure 2** above.
- **Comparison** – establishment of a link between the corresponding surfaces on the fingermark and corresponding reference fingerprint. In this step the objective is to mark the (dis)similarities in the fingermark and the reference fingerprint. The outcome usually consists of a list of well-documented (dis)similarities found during the comparison. Conclusions typically reported by fingerprint examiner at the comparison stage are fingermark being of a Value for Individualization (VID), Value for Exclusion Only (VEO). If not possible to distinguish between these two categories, the comparison can be marked as Inconclusive (INC).

The subsequent two steps are beyond the scope of the CS-SIS AFIS, but will be discussed in more detail in the "MS visits" chapter where best practice in different laboratories will be presented.

- **Evaluation** – quantification of the evidential value of corresponding features found in the fingermark and in the reference fingerprint.
- **Verification** – this term usually means a (blind) verification by additional fingerprint examiner. Different practices are adopted by different MSs depending on the severity of the crime, but in case of a match it is common practice that at least one additional examiner verifies the findings established by the first examiner.

Note: Although the authors of the report are in no position to comment on the validity of the results or question appropriateness of scientific protocols used in the publications in state-of-the-art review below we feel obliged to mention, that although the false negative rates are quoted by vast majority, the false positives rates information which is often omitted would help the interested readers to form a "greater picture".

1.1. Feature extraction and fingermark mark-up

Prior to launching a search in the fingermark ABIS, fingerprint examiners either manually, or using automatic feature extraction assisting tools mark the features in the fingerprint, which form a fingermark feature vector.

Traditionally, fingerprint examiners mark level 1 and level 2 features, which include general pattern, singularity points, minutiae. Level 3 features, such as pores, dots and incipient ridges are often considered extended features. All three levels are well documented in [4]. The survey amongst forensic practitioners performed in 2008 by Anthonioz et.al. [5] indicated, that there was no real consensus on the classification, reproducibility and individual value of level 3 features. Study published in 2012 by Indovina et.al. has however shown, that the performance of automatic recognition algorithms on fingermarks significantly increases using extended feature sets [6]. In 2013 Chapman et.al. published mark-up instructions for extended friction ridge features [7].

Important challenge is triggered by the reproducibility, repeatability and "large" inter / intra examiner variation when marking minutiae on fingermarks [8] [9] [10]. In areas where the examiner was certain about presence/absence of a minutiae in the fingermark the median reproducibility of minutiae mark-up amongst examiners was 82%, while in unclear areas the median reproducibility of minutiae mark-up was only 46% [9].

1.2. Deep learning in fingermark image processing

Deep learning algorithms and convolutional neural networks (CNNs) are finding their way into the domain of forensic fingerprints as well. Some of the applications of CNNs include image enhancement feature extraction and comparison. Given the very active academic community, it is difficult to be completely exhaustive and provide a detailed overview of latest state of the art in processing of fingermarks. Nevertheless, we tried and split the deep learning state of the art into following subsections: Image enhancement, CNN based comparison algorithms, CNN based feature extraction.

1.2.1. Image enhancement

Li et.al. in their work published in 2018 are using a FingerNET inspired deep convolutional neural network for fingermark image enhancement [11]. As highlighted in their article, the FingerNET consists of three major parts, one convolution part used for feature extraction and two deconvolution parts. The first deconvolution part is used for image enhancement (removal of structured noise) and the second one to "*guide the enhancement through multi-task learning strategy*". The deep CNN is trained in a pixel-to-pixel, end-to-end learning, which produces an enhanced fingermark at the output. Three implementation details are studied: 1) single-task learning, 2) multi-task learning and residual learning.

FingerNET is trained offline using NIST SD4 database. The CNN is not trained on the whole rolled fingerprint images. In order to better correspond to the purpose of fingermark enhancement, the fingerprints in the SD4 database are broken into 109x109px patches by overlapping at 61x61 px. This way the same fingerprint region appears in different sampling patches, which produces slightly different contextual information for each of the samples. Low quality patches and background noise (other than fingerprint itself) are excluded from the learning process using a quality mask based on reliability map thresholding.

Structured noise is introduced to the fingerprint patches using Gabor functions to add lines, and characters, which are common in fingermarks, in order to simulate "real" fingermarks. In the pre-processing stage the total variation decomposition of the fingermark into cartoon (piece wise smooth background noise) and texture (oscillatory texture – for example ridges) component is used.

NIST SD27 database is used in the "online" experiments, showing effectiveness and robustness of their method based on FingerNET. Fingermarks are pre-processed to obtain the texture components and fed to the CNN inference procedure for image enhancement and ROI mark-up.

The final network architecture consists of convolution layer (feature extraction), deconvolution layers (transpose / fractal for image enhancement), pooling (removes

noisy activations, obtains better abstraction, increases the receptive field) and unpooling (reverses the pixels back to their original location) layer and several skip connections (compensates for possible details lost in the process of deep convolution).

CNN proposed in this work outperforms the current state of the art methods (Total Variation [12] and Adaptive Directional Total Variation [13] and Localized Dictionary [14]), in some cases by a considerable margin. The advantage of the method proposed is the directly generated enhanced fingermark as an output of the FingerNET.

1.2.2. CNN based automated fingermark comparison algorithm

In their 2018 publication researchers from the MSU have used convolutional neural networks for ridge flow estimation and extraction of minutia descriptor, combined with extraction of complementary templates (two minutiae templates and one texture template) to represent the fingermarks [15]. Thus, the method described in this article presents a complex multilevel system used in fully automatic fingermark comparison. In order to retrieve a short candidate list from the reference database, the comparison scores between the fingermark and reference fingerprint are based on a fusion of all three templates.
Their experiments indicate a rank-1 identification accuracy[25] of 64,7% for the NIST SD27 database and 75,3% for the WVU database against a gallery of 100K rolled fingerprints. The performance of their CNN-based algorithm is amongst the best of the published papers and directly comparable with leading Commercial Off-The-Shelf (COTS) AFIS algorithm, which achieved rank-1 accuracies of 66,7% on NIST SD27 and 70,8% on the WVU database.
Using a score-level fusion of the algorithm proposed with the COTS AFIS the overall rank-1 accuracy identification rates improved from 64,7% to 73,3% on the NIST SD27 database and from 75,3 to 76,6%. Using a rank level fusion, the resulting rank-1 accuracy rates improved further to 74,4% on the NIST SD27 and 78,4% on the WVU database.

Although it is unclear what algorithms are used in the COTS algorithms, this work shows important added value (approximately 10% improvement on the rank-1 identification rate on both datasets) and complementarity of deep learning approaches based on CNN's with the COTS algorithms.

1.2.3. CNN based feature extraction

Detection of pores (third level features)

Convolutional Neural Networks were used in [16] to extract third level fingerprint features (the pores) in the work entitled "*a novel pore extraction method for heterogeneous fingerprint images using CNN*".
In this work the third level features, the pores, are proposed as a means of quality assessment, liveliness detection (as it is difficult to create them artificially), biometric matching for live applications and comparison of fingermarks. The method proposed for

[25] Questioned fingermark is mated with its corresponding reference fingerprint in the reference database.

pore extraction uses a specifically designed and trained CNN to estimate and refine the centroid of each found pore.

The usability of this method in forensic practice is however questionable as pores are "not very often" visible / present in the fingermarks recovered from the crime-scenes. Another downside of this method is that it requires fingermarks / fingerprint images in high resolution (800dpi+).
The outcome of the method proposed is a matrix containing cartesian coordinates of the centroids found in the fingermark/fingerprint. Overall, their approach consists of four steps in which the CNNs are employed in two tasks – CNN pore detection, estimation of the coordinates of pores, filtering and feature extraction and CNN refinement (discarding of the erroneously detected pores). The method proposed outperformed previously reported methods in the task of detection of pores.

Ridge Shape Features

In their work published in 2017, Lee et.al [17] use the ridge shape features for partial fingerprint comparison in addition to the minutiae in a multi-stage matching process. The ridge shaped features (RSFs) represent small ridge segments where particular edge shapes are observed and are detectable in 500+ dpi images. In the minutiae comparison the corresponding minutiae pairs are matched by comparing local RSFs and the adjacent minutiae. In the ridge-feature comparison stage the RSFs of the overlapping areas are further analysed to enhance the comparison accuracy.
Eight basic ridge shapes are used to describe the local ridge structures. Although these structures are more likely to be visible in higher resolution images (such as 1000DPI), they have been observed in more traditional 500dpi images.
Partial fingerprint images of various sizes (9.8x9.8mm, 8.1x8.1mm, 7.3x7.3mm) were evaluated and the method proposed (combination of RSF and minutiae matching) showed the lowest Equal Error Rate(EER) amongst a decent representative sample of other methods (Conventional Minutiae Matcher, Accelerated-KAZE, Minutiae Cylinder Code, Representative Ridge Point, Histogram of Oriented Gradients).

Methodology for partial fingerprint enrolment and authentication on mobile devices, published by S. Mathur in 2016 [18] presents a novel method based on KAZE features (multiscale texture descriptors) for fingerprint comparison. KAZE features use non-linear diffusion to perform blurring, locally adaptive to the image data, preserve the object boundaries and remove noise. This approach proves to be particularly useful when singularity points (such as core or delta) are not present in the fingerprint image and when only a "reduced-size" fingerprint image is available.
Method proposed based on Region of Interest (ROI) segmentation in combination with A-KAZE features demonstrates considerable improvement on FVC2000 and FVC2002 databases, compared to several selected algorithms (amongst other Verifinger v 7.1).
Although missing a direct comparison with a state-of-the art, the approach presented works in real-time on embedded devices.

A reliable orientation field estimation method based on sparse coding combined with dictionary learning was proposed by Liu et.al. [19] for boosting fingermark comparison performance of AFIS systems. A total variation model is used to decompose the fingermark image into its cartoon (containing for example structured noise) and texture components. Then a multi-scale sparse coding is applied the texture image to iteratively

estimate local orientation fields, in which the dictionaries were learned from orientation fields of good quality fingerprints. Noise disrupted parts "corrected" by iterative increase of the local patch sizes and overall orientation field is reconstructed.
The method proposed reaches results comparable with previous methods (Short Time Fourier Transform [20], 2nd Fourier expansion [21], Hough transform and localized dictionaries [22] [23]) in terms of average orientation error estimation. However, it significantly reduces the time needed to learn the multi-scale dictionaries in an offline mode 0.06h and to perform the fingermark orientation field estimation online <2s. Although not quantified, graphical results show an increase of performance on the good quality fingermarks from the NIST SD27 database.

Researchers from the Universita Autonoma de Madrid propose to use unusual or rare minutiae, which are not typically used by traditional AFIS systems, as extended feature set to boost their rank-list accuracy [24]. For their experiments they use mated fingermark dataset collected in real operational conditions by the Guardia Civil (Spanish law enforcement agency). The classification of the fingermarks (15 unusual / rare types), minutia mark-up and corresponding minutiae matching was done manually by fingerprint examiners for all 268 fingermarks. In the two-stage process they use least squares fitting error to find affine transformation from the fingermark set onto the 10-print minutiae set. In the second stage they use score-level fusion to modify the similarity scores generated by three different minutia-based matchers using the fitting error. Using only the proposed score fusion they improve the rank-1 accuracy from 78.15% to 92.72% using the MCC-SDK matcher. Using rare features and the score fusion the rank-1 accuracy of the MCC-SDK matcher is further improved to 96.03%.

Although the results seem impressive, it would be interesting to see how the method proposed performs on the standard datasets – such as NIST SD27. This way it could be put in contrast with research published for example in [15].

1.3. ABIS-Fingermark Accuracy Evolution

Last evaluations of vendors technology covering the topic of fingermarks was the NIST Evaluation of Latent Fingerprints Technologies (ELFT), full report published in 2011 [25] and the roadmap to this report is presented in **Figure 3** below. It should be noted, that although the last fingermark recognition vendor test has finished in 2014, the research and development in the area of automatic fingermark comparison continues.

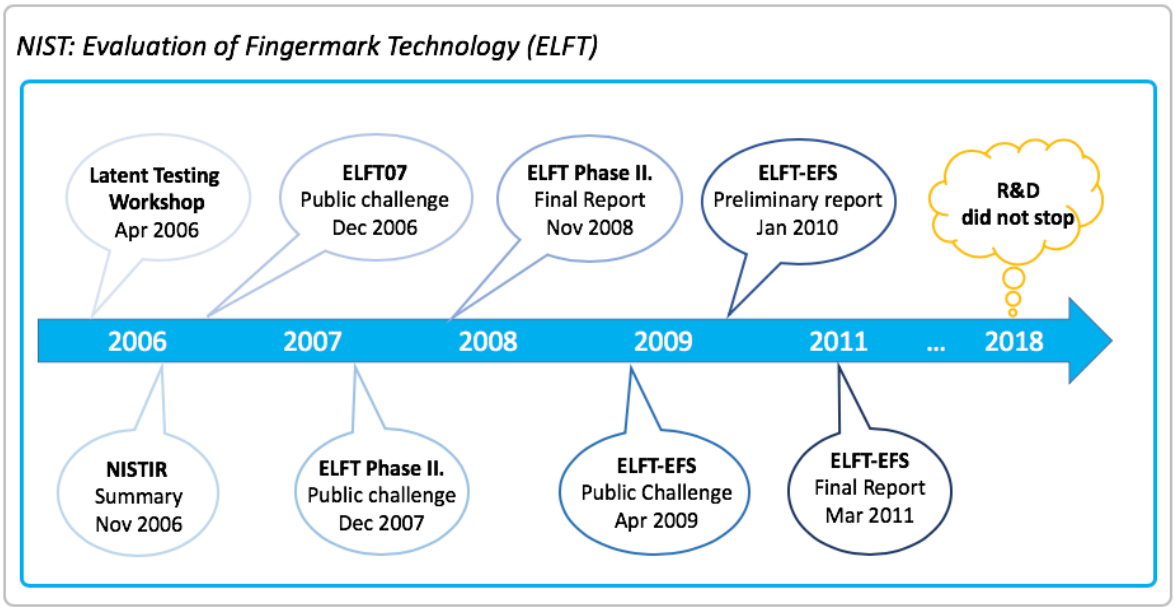
The ELFT initiative started in 2006 with the organization by NIST of a preliminary Latent Testing Workshop. The main findings can be consulted in [26]. The outcome of the workshop was summarized in the NISTIR document and led to organization of the first ELFT public challenge, which aimed to assess the core capabilities of (at that date) current automatic fingermark comparison algorithms. The evaluation consisted of two tests, run in a "lights-out[26]" environment.

[26] The term lights-out is a colloquial expression adopted by the forensic fingerprint community, which refers to a automatic processing of digital friction ridge evidence (fingermarks, palmmarks, palmprints, fingerprints). The automatic process includes feature extraction, template creation and comparison against a reference database.

"lights-out", a fully automatic fingermark process assumes no human intervention. Two tests, labelled as Phase I and II were performed. The main purpose of the proof-of-concept Phase I was to demonstrate functionality of the software in a lights-out environment. During Phase I the software was set to demonstrate:

- automated feature extraction from fingermarks;
- automatic comparison against 10-prints stored in the database;
- generation of candidate lists.

Figure 3. Roadmap to the Evaluation of performance of Fingermark Technology (Source: EC 2018)



A significantly larger database was used in Phase II to evaluate the performance for automated searches. All the tests and results carried out in Phase II are detailed in [27], where the best performing algorithm over 500 dpi images obtained a Rank 1 accuracy of 71.4% in the database of N=100.000 identities (10-prints).

The ELFT initiative continued in 2009 with the organization of a second workshop and with the announcement of a second evaluation in a "semi lights-out" environment. In this case some level of human intervention was allowed (at the level of feature extraction), however the comparison process was again fully automatic. The main purpose of this evaluation was to assess the accuracy of "lights-out" comparisons of fingermarks using features marked by experienced human fingerprint examiners. A key result of the test was to determine the conditions, under which the human minutiae mark-up is effective. As human mark-up is expensive in terms of time, effort and expertise, there is a need to know when image-only searching is adequate and when the additional effort of marking minutiae and extended features (e.g. sweat pores, core, delta) is appropriate. The results of Phase II of the ELFT challenge were published in November 2008.

The second part of the ELFT report, entitled Extended Feature Sets (Evaluation #2) was released in April 2012 [6]. Unfortunately, the data used in 2009 ELFT-Phase II and the data used in 2010 ELFT-Extended Feature Sets were different, which deems the results

not comparable. In the 2012 human-aided evaluation, the Rank 1 accuracy of the best system was 62.2% over a search database of *N*=100.000 identities.
Fingermarks of "higher" quality, not strictly representing the "day-to-day" casework were used in the NSIT 2006 ELFT Phase II.

In their work published in 2018 [15] researchers from the MSU performed experiments using the CNN's for ridge flow estimation and extraction of minutia descriptor, combined with extraction of complementary templates (see section 1.2.2). Their CNN based fingermark comparison algorithm achieved comparable results to the COTS algorithms and using a score-level fusion with the COTS AFIS the overall rank-1 accuracy identification rates improved from 64,7% to 73,3% on the NIST SD27 database and from 75,3 to 76,6%. Using a rank level fusion, the resulting rank-1 accuracy rates improved further to 74,4% on the NIST SD27 and 78,4% on the WVU database.

Additionally, continuing this line of latent performance evaluation, in 2013 NIST made public a presentation by the Federal Bureau of Investigation (FBI) which gives selected statistics on State and Federal Agency fingermark searches. The document also discusses methods for improving performance (individualization) for latent searches and covers steps toward greater automation in the future, such as increased reliance on image-only searches [28].

Several conclusions can be drawn from the ELFT evaluations. Perhaps the most important ones are:
1) High quality fingermarks are AFIS searchable in the "fully lights-out" mode;
2) Reliable quality metric is necessary to assist the fingerprint examiners in the determination of quality of the fingermarks.

The NIST Fingerprint Vendor Test Evaluation FpVTE 2012 (full report published in December 2014) did not cover the fingermark identification use-cases. Interested readers are kindly referred to [29].

1.4. Evaluation of performance of fingerprint examiners

Although this section is not a mandatory pre-requisite for the CS-SIS (it is assumed that only Value for Comparison (VC) fingermark images will be submitted for comparison) it is important to highlight, that the assessment of fingermarks image quality, due to the absence of NFIQ2-like quality metrics for fingermarks, is left solely at the discretion of trained fingerprint examiners.

Since the quality of the fingermarks found on the crime scene is questionable and the process deposition of fingermarks on wide variety of surfaces non-repeatable, the involvement of fingerprint examiners in many different aspects of the ACE-V protocol is unavoidable. Their opinions therefore matter and their opinions, as well as evaluation of their performance have been subject to extensive studies in the past [8] [9].
Following an erroneous identification of a fingermark in the Madrid bombing [30] in 2004 the FBI review committee recommended (amongst others) a study of the performance of fingermark examiners [31]. The evaluation of accuracy of fingerprint examiners was further highlighted by other institutions [32] [33] [34].

Study of Ulrey et.al. from 2011 [35] presents results of the first large scale study including 169 fingermark examiners' decisions in terms of accuracy and reliability. In this study each of the 169 fingerprint examiners compared 100 fingermarks and the corresponding fingerprint from total of 744 fingermark-fingerprint pairs. Median experience of the fingerprint examiners was 10 years of expertise and 83% examiners were certified fingerprint examiners.

Fingermarks were selected to best reflect the variety of different aspects and quality to reflect the forensic casework. In terms of accuracy, five examiners made false positive error (FPE) which translated in FPERR of 0.1%, while 85% of examiners made at least one false negative error (FNE) resulting in FNERR of 7.5%. The study was completed with a non-surprising conclusion of "*examiners frequently differing on whether fingermarks were suitable for reaching a conclusion*". In the course of fingerprint evidence evaluation, the examiners were requested to determine the value of fingermarks and were allowed to attribute fingermarks to 3 categories in the analysis phase: 1) Value for Identification (VID), 2) Value for Exclusion Only (VEO), 3) No Value (NV). The conclusions reported by the examiners in the comparison phase were: 1) Individualization (ID), 2) Exclusion (EX) or 3) Inconclusive (INC).

Subsequent study by Ulrey et.al. from 2012 [12] focuses on repeatability and reproducibility of decisions made by the fingermark examiners. Intra-examiner repeatability was studied on the pool of 72 examiners, who participated in the previous study and were re-tested after approximately 7 months. Inter-examiner reproducibility was derived from the previous study [35].

Examiners repeated 89.1% of their individualization and 90.1% of their exclusion decisions. Repeatability of comparison decisions (ID, EX, INC) was 90% for the fingermark-fingerprint pairs and 85.9% for non-mated pairs. None of the false positive errors were made, while 30% of false negative errors were repeated. The study concludes that: *"… much of the variability appears to be due to making categorical decisions in borderline cases."*

In summary, experts' opinions, from whichever angle we look at them, are subjective and their decision-making processes may be influenced by many factors. Recently two black and white box studies have been published [36] [37].

1.5. Fingermark crowd-based learning

The power of crowd was used in several publications, mainly to understand and highlight the differences in the minutiae mark-up by different fingerprint examiners. The opinions and expertise of fingerprint examiners were in the past used to assess the pertinence of the features in fingermarks, analyse different features marked by different examiners and consequently, to use the knowledge of crowd to predict the value of fingermarks with respect to the performance of the ABIS-fingermark. The knowledge of the crowd of experts can be considered as an input parameter in the process of development of fingermark image quality metrics.

Inter-examiner variation of minutia mark-up on fingermarks

In their 2016 publication [9], Ulrey et.al. assessed variability in minutiae mark-up among 170 volunteer fingerprint examiners. Each of them marked minutiae on 22 randomly assigned fingermark and corresponding fingerprint pairs out of the pool of 320 fingermark-fingerprint pairs. On average, 12 fingerprint examiners marked each fingermark-fingerprint pair. Although similar minutiae counts were reported, the mark-ups varied greatly with respect to which specific minutiae were selected.

One of the primary factors associated with the reproducibility of minutiae mark-up was the fingermark image clarity, regions examiners chose to work on and agreement on value or comparison determinations. The median minutiae mark-up reproducibility in clear areas was 82%, while in unclear areas it dropped to 46%. Low reproducibility was likewise associated to differences in value or comparison determinations.
Several factors were identified, which affected the minutiae mark-up reproducibility – image clarity, region of interest, type of features and location.

Crowd Powered Fingermark Identification: Fusing AFIS with Examiner Mark-up

Crowd-powered fingermark identification framework, in which multiple fingerprint examiners work in conjunction with AFIS to boost the overall performance of the AFIS was proposed by Arora et.al. in 2015 [10].
In this work, the candidate list provided by AFIS for each marked fingermark was used to determine the likelihood of a rank-1 hit. A fingermark for which this likelihood is low was crowdsourced to a pool of fingerprint examiners for future mark-up. The mark-ups (minutiae feature vector) is then input into the AFIS to increase the likelihood of producing a HIT in the reference database.
Experimental results have shown that fusion of examiner mark-ups with AFIS improves the rank-1 identification accuracy by 7.75% using six mark-ups on the 500ppi NIST SD27 DB, by 11.37% using two mark-ups on the 1000ppi ELFT-EFS public challenge database and by 2.5% on the 1000ppi RS&A database against the 250.000 rolled prints in the reference database using a single mark-up.

Fingermark Value Prediction: Crowd-based learning

Crowdsourcing was used in a framework proposed by Chugh et.al. in 2018 for Fingermark Value Prediction [38]. The values in question are Value for Identification (VID), Value for Exclusion Only (VEO) and No Value (NV), which are values typically used by fingerprint examiners in the analysis part of the ACE-V procedure.

Experimental results are reported using four fingermark datasets (NIST SD27, MSP, as well as WVU and IIITD) and state-of-the-art AFIS. Major limitation of the LFIQ quality metric, deemed in this work is the necessity of minutiae annotation as one of the input parameters. Another potential limitation of the previously proposed quality metrics is that the target predicted fingermark value was most of the time based on single examiner (or very limited number of examiners) annotations.

In order to address the above-mentioned limitations, the authors have developed a crowdsourcing tool FingerprintMash, which was used to collect the inputs from the expert

crowd. The Multidimensional Scaling (MDS) was used to identify the bases that explain the inter-examiner variations.

In the crowdsourcing exercise quality labels (corresponding to the NFIQ values) were assigned by the pool of experts (31) to a set of randomly selected 100 fingermark pairs from a database of 516 fingermarks. In total they obtained 3.100 quality labels for pairwise comparisons and overall 6.200 quality labels. In the next step the Crowd Reliability was evaluated and the Inter-Expert Variations analysed. In order to interpret the MDS scaling, the bases were explained in terms of fingermark features (19 features were automatically extracted from each fingermark). Lasso was used to learn the fingermark value predictor (to model the relationship between the MDS bases and the expert assigned fingermark value).
Several major contributions were achieved in this work: 1) design and implementation of crowd-based framework, 2) MDS scaling used to identify underlying bases expert fingermark value assignment, 3) establishment of a link between the automatically extracted fingermark features and MDS bases using Lasso and 4) learned the predictor based on underlying bases to assign a value to a queried fingermark.

1.6. Fingermark Datasets

What makes "reliable" fingermarks datasets particularly difficult to come by is the added value of availability of their mated corresponding fingerprints – rolled or flat. Thus, although the sets of fingermarks and mated fingerprints in principle exist in every MSs forensic or crime investigation unit, they are typically not publicly available. An overview of publicly available datasets is presented below in **Table 2**.

Once a fingermark is individualized (suspect reference fingerprint found), the fingermark and the matched fingerprint pair are (can be) stored in a "resolved case" database. MSs maintain these datasets for future reference, serving the purpose of evaluation of performance / benchmark of their fingermark ABIS. Since fingermarks are collected and analysed in the scope of police / crime scene investigation, the corresponding datasets are managed by the police forces. It is therefore very difficult to gain access to these datasets.

In the past, NIST has made available two datasets containing the fingermarks and reference fingerprints, which were used in vast majority of the experiments and scientific publications. The "special database" SD27[27] (consisting of 258 fingermarks and reference fingerprints with level 1 and level 2 features manually marked by fingerprint examiners) and its later version "special database" SD27a. At the date of publication of this report the NIST SD datasets have both been discontinued. According to the information available on the NIST website, they are currently working on the replacement of the SD27a.

Another dataset, referenced in some of the reviewed articles above belongs to the West Virginia University (WVU). The WVU latent database[28], which consists of 449 fingermarks and mated reference fingerprints and is publicly available.

---

[27] *NIST Special Database 27*, https://www.nist.gov/itl/iad/image-group/nist-special-database-2727a

[28] *Integrated pattern recognition and biometrics lab, West Virginia University*

Several different datasets are available under license (subject to agreement) via Image analysis and Biometrics Lab of the Indraprastha Institute of Information Technology, Delhi. Their multi-surface latent database consists of 551 fingermarks from 51 subjects lifted from different surfaces (ceramic plate, mug, glass, steel glass, CD, plastic CD cover, paperback and hardbound book covers). Mated reference fingerprints are captured for each subject using a live scan device at 500dpi. Their fingermark database contains a collection of 1046 fingermarks lifted from card and tile from all fingers of 15 subjects. Multiple fingermarks are captured for every corresponding fingerprint, thus enabling the LP-LP comparison. Reference flat fingerprints are recorded at 500 and 1000dpi resolution.

Table 2. Overview of publicly available fingermark databases

Database name	# identities	#palmprint imgs	Reference	Available
NIST SD27	unknown	258 mated fingermarks	500dpi	Discontinued
NIST SD27a	unknown	Mated fingermarks		Discontinued
WVU latent	unknown	449 mated fingermarks	500dpi	Yes (subject to agreement)
IIITD multi-surface	51	551 mated fingermarks	500dpi lifted from 8 different surfaces	Yes (subject to agreement)
IIITD latent	15	1046 mated fingermarks lifted from 2 different surfaces	Flat fingerprints at 500 and 1000ppi	Yes (subject to agreement)

1.7. FBI – NGI fingermarks [29]

At the date of publication of the assessment, there were approximately 400K fingermarks stored in the IAFIS ULF database, mainly provided by the FBI laboratory division and federal state partners. In the past, the fingermarks were searched only against a best set of fingerprints 10-Prints (TP) cards (IAFIS Criminal Master File). In the NGI, the fingermarks are searched against all fingerprint evidence (rolled, flat, slap) with the possibility to choose repositories and identity groups within the NGI to be searched, including search against civil submissions (if permitted by the authorities and requested by the contributing party).

All incoming criminal TP cards are searched against the ULF. Incoming "to be recorded" TP cards are searched against the ULF, while the choice of not to search against the ULF is given to agency submitting the "not to be recorded" TP cards. Automatic notification regarding a hit on the ULF is sent only to the "owner of the fingermark" (agency supplying the fingermark). All supplementary fingerprint evidence (rolled whole finger, rolled tip of

[29] CJIS/FBI, Privacy Impact Assessment for the Next Generation Identification (NGI) Palm Print and Latent Fingerprint Files, 2015 https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/next-generation-identification-palm-print-and-latent-fingerprint-files

a finger) accompanying the TP file or having an identification number are recorded and searched against the ULF.

Section 1. Summary of key concepts

- The last large-scale public challenge on fingermark recognition was performed in 2009. Since then the automatic fingermark recognition technology saw a significant increase in rank-1 accuracy, also thanks to the advances in deep learning and adoption of convolutional neural networks.

- Deep learning-based approaches have led to improvements in the domain of automatic fingermark image enhancement, which subsequently led to more robust and reliable minutiae detection and detection of extended features (ridge shapes and pores).

- The use of extended feature sets provides additional boost in terms of improved accuracy of ABIS-fingermark systems.

- Key fingermark datasets are very difficult (if not impossible) to get hands on a mated fingermark dataset with known ground truth for the R&D purposes.

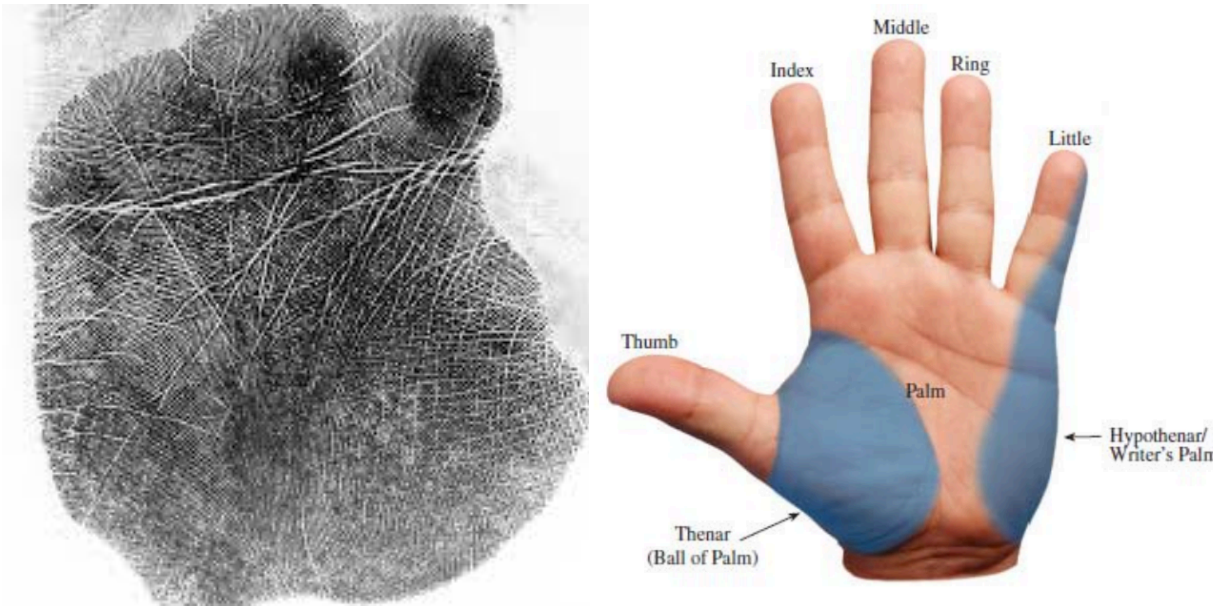
- Fingermark analysis, comparison, evaluation and verification are in the competence of skilled fingermark examiners. Quality of fingermarks is assessed subjectively on a case-by-case basis and only fingermarks showing value for comparison (VC) in the analysis phase make it to the subsequent stages.

2. ABIS-Palmmarks, Partial Palmprints and Palmmarks Technology

Nowadays, it is a common practice to capture the impressions of palms (palmprints) in the course of booking of persons (subjects to criminal investigation), in addition to the capture of fingerprints (rolled and/or flat). In some countries it is common to capture also the hypothenar area of the hand, known also as the "writer's palm" (opposite of the thumb on the outer extreme of the palm) in the booking process.

High resolution (minimum 500 or 1000ppi) palmprint images are recorded when a person is booked at the police station (see **Figure 4** below). Lesser resolution has been deemed not usable for the purpose of identification, as the general patterns, singularity points and minutiae points are usually not visible.
As in the case of fingerprint ten-print cards, they can either be acquired using live-scan devices (digital) or in a form of "inked and rolled" impressions deposited on a paper palmprint card (a process nicely illustrated in [39] – chapter 4.3.2). The palmprint cards are subsequently digitized using high resolution scanners in order to become suitable for further automatic processing.

Figure 4. Palmprints. Left: High resolution palmprint[30], Right: image writer's palm[31].



[30] Image source: Carreira, L., Correia, P.L., Soares, L.D., *On high resolution palmprint matching*, Int. Workshop Biometrics Forensics, Valletta, Malta, March 2014, pp. 1-6

[31] https://www.fbi.gov/file-repository/guidelines-for-capturing-palm-prints-and-supplementals.pdf/view

2.1. Comparing Palmprints

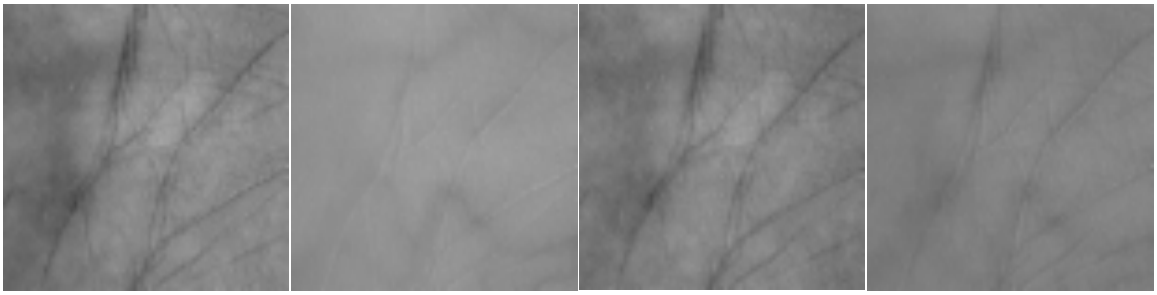
Due to their considerably larger surface area, the process of comparing palmprints presents bigger challenges than the process of comparing fingerprints. From the point of view of throughput (processing time) of the palmprint comparison algorithms, two different approaches can be found in the literature:

- Online comparison
- Offline comparison

2.1.1. Online palmprint comparison

In the online comparisons, as the title suggests, the processing of the palmprints occurs in real time. For this purpose, the palmprints can be acquired either using touch-based or touchless palmprint sensors. The online processing capabilities are guaranteed thanks to use of low resolution (<100dpi), very often multi-spectral images of full palmprints (see **Figure 5** below). Due to the low resolution of the images, the online palmprint comparison is more suited for 1:1 verification and identification in closed sets or in small rather than for identification in the scope of police investigation.

Figure 5. Examples of low resolution partial palmprints typically used in online palmprint comparison (full spectrum, R, G, B) (examples of multispectral database referenced in [10])



Although not the main focus of this study, for the sake of completeness we mention few of the most recent approaches featuring traditional and novel methods from the machine learning: autoencoders with regularized extreme machine learning [40]; quarterion principle component analysis [41]; LHEAT and the IFkNCN Classifier [42]; palm code introduced in [43]; multiclass projection extreme learning machine and digital shearlet transform [44]; image fusion for illumination invariant palmprint recognition [45]; local binary pattern histogram, Fourier features and Gabor filter [46]; oriented multiscale log-Gabor filters [47]; hierarchical approaches [48], histogram of oriented gradients (HOG) [49] or a combination of these.

Various different classification algorithms are used to discriminate between genuine users and impostors[32], ranging from traditional ones like Support Vector Machines (SVM),

[32] Genuine and Impostor users (or trials) are in the harmonized biometric vocabulary referred to as mated (probe and reference originate from the same-source) and non-mated (probe and reference originate from different-source) comparisons.

Euclidean distance, KNN, random forests or convolutional neural networks (to name a few).

In one of the most recent articles [40] the reported accuracy for their proposed online system on a closed set of 3000 palmprint images (2x250x6 training and 2x250x6 testing images from of the MS-PolyU database[33] per spectrum (R, G, B and NIR) reported accuracy of 100%[34] for some of the spectra. In some applications, low resolution palmprint image recognition is fused with palm-vein image recognition in an attempt to provide more secure 1:1 identification and authentication methods [50] [51].

2.1.2. Offline palmprint comparison

The term offline is based on the actual physical size of the palmprint images, which in this case are of a high resolution (common are 500, 600 or 1000dpi).
High resolution palmprints share some common characteristics with the fingerprints recorded in a form of TP cards. In the 500dpi palmprints second level features, such as minutiae points (bifurcations and line endings), singularity points and ridge details, are visible; while in the 1000dpi images, depending on the overall quality of the image, pores (sweat glands) can be observed. Apart from these, the shape and position of palmar creases presents additional important discriminative feature.
The main challenge in the development of a reliable automatic palmprint recognition system is the presence of creases, large nonlinear distortion present in the palmprints due to the nature of capture of the palmprint images), large image size and from it derived high computational complexity necessary to process and match the palmprint images. Not to mention the non-availability of high resolution palmmark and palmprint image databases due to the fact that these are mainly produced and owned by the law enforcement agencies.

2.1.3. ABIS-Palmmarks Use Cases in the context of CS-SIS

For the purpose of currently allowed use of palmprints in the CS-SIS with respect to the article 40 – serious crime and/or terrorist activity – the main focus of this literature study will be on the forensic applications. However typical use cases can be summarized in the following:

- Full-to-full palmprint search, an equivalent of 10-print vs 10-print (TP-TP) search in fingerprints
- Partial-to-full palmprint search, an equivalent of single finger (or a fingermark) vs 10-print search in fingerprints
- Palmmark-to-full palmprint search, an equivalent of fingermark vs 10-print search

From the year 2000 onwards, palmprint feature extraction and comparison algorithms derived from fingerprint feature extraction and comparison algorithms can be found in the scientific literature, which is logical, given that some of the features are fairly similar.

[33] See section Palmprint Databases below.

[34] The reader is kindly reminded that this accuracy is achieved on a closed set with low resolution palmprints.

2.2. Comparing High Resolution Palmprints

From the image quality point of view, the overview of palmprint comparison techniques for 1:N identification purposes starts with "relatively" easiest scenario – comparing full to full palmprints. The term "relatively" is in place, as unlike in fingerprint comparison, full palmprints contain a LOT more information. Taking the simplest minutiae-based comparison approaches as an illustrative example, number of minutiae in fingermarks in the NIST SD27 database range between 5 and 86. Average number of minutiae in flat fingerprints is comparable to that upper bound and number of minutiae in a rolled fingerprint slightly higher (due to the surface area being larger than in the case of the flat fingerprint). On the other hand, the reported average number of minutiae of full palmprints in the THUPALMLAB database is 879 [52]. Even in case of using the same comparison algorithms as in the case of fingerprints, the computational complexity (and time) necessary to perform the comparisons significantly increases for palmprints.
Several different approaches have been reported in the scientific literature: minutiae based and minutiae-based plus feature-based comparisons.

2.2.1. Minutiae-based full-to-full palmprint comparisons

Early approaches can be labelled as "minutiae-based". Although researchers from different teams used different methods, the minutiae-based approaches have following parts in common:

- image segmentation (including orientation field estimation)
- image enhancement (noise removal, binarization)
- feature extraction (skeleton, extraction of minutiae feature vector composition)
- feature comparison (local similarities, local comparison, segment fusion, final comparison score)

Researchers at the Nankai Institute of Machine Intelligence were amongst the first with recorded publications, covering the topics of image segmentation, image enhancement, feature extraction and post processing [53] [54] [55] [56] [57] and in 2009 published their first offline minutiae-based palmprint identification system [58]. They reported a rank-1 identification rate of 59,02% (mainly due to the nearest neighbour-based approach used) in 1:N identification task to find 49 high resolution palmprint images in a database of 9600 full palmprint reference images (4800 individuals, 500 dpi images, 2304x2304px, 256 greyscale, belonging to the Institute of Criminal Technology in P.R. China).

Minutiae-based full-to-full palmprint recognition system was developed by the Michigan State University (MSU) and published in a form of technical report entitled *"On palmprint matching"* [59]. In their work the palmprint segmentation stage was succeeded by the contrast enhancement stage, the feature extraction stage (creases and minutiae) and finally minutiae comparison. The comparison stage consisted of palm alignment, sector definition (5 sectors), sector-wise comparison and finally a score level fusion in which resulting scores of all sectors were combined. The accuracy reported reached 98,9% FAR at 0.01% on their in-house database of 100 palms (50 individuals) with 10 impressions per palm.

Different system, yet still minutiae-based was proposed in 2012 by the researchers from University of Bologna [60]. This publication was inspired by their previous work on

minutiae-cylinder-code (MCC) in the area of fingerprint recognition, in which a local structure is associated with each minutia. They applied a local comparison strategy on the MCC representation followed by a relaxation procedure in order to obtain a global resulting comparison score (see [60] for more details). Overall, they reported EER < 0.1% at an average speed of < 2s for feature extraction and < 0.04s for comparisons on a THUPALMLAB database.

2.2.2. Minutiae and feature based full-to-full palmprint comparisons

Minutiae-based features have been complemented by a density map, creases line map and orientation field in the research published by the group at the Tsinghua University [61]. Among other, they proposed a novel method invariant to presence of creases developed for orientation field estimation and a novel fusion scheme. They reported 4.8% EER and a rank-1 identification rate of 91.37% on the THUPALMLAB database at a cost of reported 67s for feature extraction and <5.2s for comparison.

In the subsequent work Dai et.al. published update of their previous system in 2012 [62], in which they use registration algorithm based on orientation field to cope with different positions and orientations of palm-prints. In their work they propose a segment-based palmprint comparisons and cascade filtering, which allows for early elimination of non-matching palmprints and thus reducing the computational complexity. The full palmprint is divided into smaller segments which are subjected to individual comparison and the final similarity score between two palmprints is computed using Bayesian framework. The system achieves reported 97,9% TPIR with the FPIR set at 2x10-3 in a task to identify 840 full palmprints in a gallery consisting of 13,736 full palmprints. Average comparison speeds reported for genuine and impostor attempts are 161ms and 39ms respectively.

"Singular points" were proposed as features complementing the minutiae-based approach for speeding up the comparison of high resolution palmprint images [63]. The "singular" points are extracted automatically from the entire palmprint and a geometrical triangular local structure is constructed for each of these points using local minutiae within a certain radius[35]. Local structures of singular points of the same type are compared in different palmprints to establish whether points compared originate from the same palm. Experiments were conducted on the THUPALMLAB database with the reported EER ranging from 4,09% to 6,51% (depending on the size of the radius).

2.2.3. Comparing High Resolution Partial Palmprints / Palmmarks to Full Palmprints

Although in principle the palmmark and partial palmprint comparison process is the same, it is important to make a distinction between these two.

The term partial palmprint refers to a cropped portion of a high resolution palmprint presenting good level of detail in a scenario. A typical scenario would be a hand which

[35] Although the units used to define the radius are not explicitly mentioned (assumed distance in *px*), the idea of reducing the amount of minutiae-to-match from ~1000 per high-resolution palmprint to "*n*" surrounding the singular point sounds intriguing. Furthermore, geometric configuration of these points (if more than 3) could potentially be exploited as "additional feature".

has suffered an injury (e.g. severe cuts) present in the thenar region, which would render the thenar part of the palmprint useless for identification, while the unaffected hypothenar and interdigital region could serve the identification purpose.

The term palmmark refers to a trace evidence recovered from the crime scene, for example a latent palmprint which was made visible and which resolution and level of visible details is questionable.

Based on this distinction, the palmmarks (same as in the case of fingermarks) will show higher level of distortion, lesser quality, lesser ridge clarity and typically smaller surface when compared to palm-marks cropped in "controlled conditions".

In the same work [62] Dai et.al. presented the capabilities of their proposed palmprint recognition system when dealing with partial palmprints. Partial palmprints used were crops from full palmprints into three major regions – thenar, hypothenar and interdigital. In total they evaluated performance of their system on 2,520 partial palmprints, which were compared against the database of 13,736 full palmprints with 91,9% TPIR (FPIR set to $5x10^{-3}$).

The palmprint recognition system presented in [59] covering full-to-full palmprint comparison covered above, included a method for partial palmprint comparison. In the first step the Region of Interest (ROI) was selected in the full palmprint templates, to match the specific partial palmprint (or palmmark) queried under the assumption that the query partial palmprint originates from a specific region of the palm (interdigital, thenar, hypothenar). These regions are automatically detected. In the subsequent feature extraction phase the crease lines, Scale Invariant Feature Transformation (SIFT) features and minutiae are extracted. In the comparison stage the SIFT features and minutiae of two images are compared and both resulting comparison scores fused.

The rank-1 identification rate of their system is 96% (comparing 500 synthetic palmprints against 100 full palmprints) and 82% on a partial palmprint dataset counting 240 images (10 subjects x 2 palms x 12 partial images). Couple of drawbacks of this study are the computational complexity for obtaining the SIFT features as well as the fact that the SIFT features may not be always be present in the palmmarks.

In their subsequent work Jain and Feng presented a dedicated palmmark-to-full palmprint recognition system [64]. For a robust minutia extraction, they proposed a region-growing algorithm, which deals with creases and reliably estimates the ridge direction and ridge frequency in a sine-wave representation of a local ridge block. They also proposed a MinutiaCode, a fixed-length minutia descriptor, which alongside the neighbouring minutia captures also ridge information.

They evaluated the performance of their comparison algorithm on 150 lives-can partial palmprints and 100 palmmarks from real cases, against a background database of 10,200 full palmprints with a rank-1 identification rate of 78.9% for the live-scan partial-palmprints and 69% for the palmmarks.

MSU palmmark recognition system was updated in 2013 [52] in three principal stages:

- training phase (K-means clustering algorithm used to obtain a set of cluster centroids)
- registration phase (minutiae and descriptors extracted and clustered from the full palmprints in accordance with the centroids obtained in the previous phase)
- comparison stage (same way of obtaining minutiae and descriptors with a small number of minutiae selected per cluster and fed through the cluster comparison procedure)

Overall, the performance of this system improved and achieved 79,4% rank-1 identification rate on 446 palmmarks in a background database of 12,489 full palmprints, with the EER of 0,11% on the THUPALMLAB Database.
A radial triangulation based palmmark recognition system [65] was proposed by Wang et.al. This research was inspired by the radial triangulation used in forensic fingerprint recognition published earlier. In their work they propose a three-step local minutiae comparison based on the radial triangulation: selection of local N-minutiae sets, radial triangulation feature extraction, and comparison of two radial triangulation structures (palmmark and full palmprint). Multiple system configurations were evaluated and the best performance achieved was 62% rank-1 identification rate on a database of 22 palmmarks and 8680 full palmprints.

Low computational complexity, minutia translation and rotation invariant partial palmprint recognition system based on regional fusion using spectral minutiae representation (SMC) was proposed in [66]. The authors proposed to divide the full palmprint into smaller regions (thenar, hypothenar and interdigital) coupled with anatomically inspired regional fusion. Both, manual and automatic segmentation approaches are used to split the palmprints into the three regions of interest. The SMC is applied in a region-to-region comparison and a regional level score fusion using the sum rule and logistic regression. From the results obtained in a region-to-region comparison it is observed, that the comparison algorithm proposed performs better on the hypothenar and interdigital regions and worse on the thenar region. Significant performance improvement is achieved in a regional fusion using both – manually and automatically segmented regions. Using the automatic segmentation, the authors report overall 2.4% EER using the sum rule fusion and 1.77% EER using the logistic regression-based fusion on the 680 palmprint subset of the THUPALMLAB database.

2.3. Palmprint Datasets

Although many different datasets were used in the state-of-the-art review mentioned above, only handful are publicly available, as shown below in **Table 3**. For the sake of completeness, one of the low-resolution public databases is listed as an illustrative example. Where available, reference to the scientific publication in which more details can be obtained is provided.

Table 3. Available palmprint databases

	# individuals	# palmprint imgs	Comments	Available
LPIDB v1.0 [67]	unknown	380 palmmarks of 100 palms	500dpi, publicly available	Yes
THUPALMLAB [68]	80	1280 palmprints (two palmprints per individual, 8 impressions per palm	500ppi, 2040x2040 px, 256 greyscale; 120x8 live-scan (Hisign palm) - available 13,616 inked & scanned palmprint images – this part NOT available	Yes
BICT [65]	unknown	22 palmmarks 8680 palmprints	500ppi	No
RS&A [52]	unknown	346 palmmarks 88 palms	500ppi	No
Noblis [52]	unknown	46 palmmarks 8 palms	Full palmprints at 1000ppi	No
MSP [52]	unknown	54 palmmarks 22 palms 9,701 full palmprints	Palmmarks 400ppi Palmprints 1000ppi	No
MSU live-scan [52]	unknown	116 palmprints (100x10 impressions + 16x1)	Full palmprints 1000ppi	No
MS-PolyU Resolution <100dpi Not suitable for identification	250	240K multispectral	Two recording sessions, 55 female, 195 male; Both palms; Four illuminations: R,G,B & NIR spectrum	Yes

2.4. MS National ABIS-Palmmark systems

In the scope of criminal investigation, palmprints are usually enrolled together with the set of suspects' fingerprints (rolled and flat).

Although full-to-full palmprint comparison is technically feasible and supported by MSs national AFIS systems, fingerprint comparison is given priority for identification of an individual. Indeed – if a full palmprint (or a set of full palmprints) of an individual is available, his fingerprints are also available.

If a suspect is booked and the palmprints are enrolled, these are searched against the database of Unsolved Latent Files (ULF) together with the suspects' fingerprints.

Palmprint databases are typically searched in the following use-cases:

- Palmprint (of a high quality) to ULF search (**PP → LP**)
- New friction ridge impression introduced into the AFIS, when it not clear whether it is a fingermark or palmmark, to full palmprint search (**LP → PP**)

2.5. FBI – NGI system Palmprints[36]

In January 2015 the FBI issued a Privacy Impact Assessment for the Next Generation Identification (NGI) Palm Print and Unsolved Latent Files. In their study the Criminal Justice Information Services (CIJS) division of the FBI highlighted the importance of the palmprints as forensic evidence by including the National Palmprint System (NPPS) into the FBI's NGI.

From the organizational point of view, NGI accepts three different types of palmprints:

- Known palmprints with fingerprints
- Known palmprints without fingerprints (but with an identifying number)
- Unknown palmprints

In first two cases the palmprints are enrolled in the NGI and placed in the corresponding group – civil or criminal. Majority of the palmprints are submitted to the NGI electronically, either by using live-scan devices or in a form of a scanned document. Prior to enrolment, every new set of palmprints is searched against unsolved latent files (ULF) containing both – fingermarks and palm-marks, unless the submitting agency chooses not to run this search.
Unknown palmprints (palmmarks), marks collected at the crime-scene or partial palmprints are likewise accepted by the NGI. Incoming palmmarks are searched in a similar way as fingermarks. This search results in a list of candidates, whose profiles (and palmprints) are returned to the forensic examiner, thus not resulting in the "positive identification", but serving the purpose of an investigative lead. Palmmarks are kept on record by the NGI as long as the submitting agency notifies the NGI about a positive identification, or opts chooses not to store the submitted palmmark. Palmmarks which are not stored are deleted, unless specifically requested by the submitting agency.

Although palmprints are generally (in the USA) accepted for positive identification, the NGI searches result in a list of candidates, thus providing an investigative lead which requires further attention of the forensic examiner. Returning file for the submitting agency contains amongst others the identification number of the candidate, candidate images, event information, comparison score.

[36] CJIS/FBI, Privacy Impact Assessment for the Next Generation Identification (NGI) Palm Print and Latent Fingerprint Files, 2015 https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/next-generation-identification-palm-print-and-latent-fingerprint-files

Section 2. Summary of key concepts

- To the knowledge of the authors, no public palmprint / palmmark recognition challenge has been organized to date of publication of the report.

- Automatic palmprint recognition technology faces additional challenges in terms of size of the palmprints. Palmprint feature extraction and comparison are more computationally intensive and more time-consuming.

- Palmprint / palmmark recognition technology is following the developments in the field of fingerprint / fingermark recognition.

- Palmprint recognition has been introduced as in some cases it is not possible to distinguish what type of friction ridge was at the origin of the dactyloscopic trace recovered from the crime scene. According to the latest reports from the use of NGI (USA) and the statistics produced by the CJIS, some 30% of dactyloscopic traces found on the crime scenes in the USA account for palmmarks.

- Fingerprint and palmprint databases are not equally populated and not equally used amongst the different MSs visited.

- Other friction ridge impressions, not mentioned in this report, are used in some cases in the scope of forensic investigation – the hypothenar region of palm and footprints.

3. Fingermark, Palmmark and Palmprint Image Quality Metrics

Many studies and benchmarks have shown that the accuracy of biometric systems heavily depends on the quality of the acquired input samples [69] [70] [71]. If quality can be improved, either by sensor design, user interface design or by complying to an (inter)national standard, better accuracy will be obtained. For those aspects of quality that cannot be designed-in, an ability to analyse the quality of a live sample is needed. This is useful primarily in initiating the reacquisition from a user (if the use-case allows), but also for the real-time selection of the best sample, and the selective invocation of different processing methods. That is why quality measurement algorithms are increasingly deployed in operational biometric systems.

Biometric quality measurement has vital roles to play in improving biometric system accuracy and efficiency during the capture process (as a control-loop variable to initiate reacquisition), in database maintenance (sample update), in enterprise wide quality-assurance surveying, in invocation of quality-directed processing of samples and even in security-related tasks [70] [71]. Neglecting quality measurement will adversely impact the accuracy and efficiency of biometric recognition systems (e.g. verification and identification of individuals). Accordingly, biometric quality measurement algorithms are increasingly deployed in operational systems. These elements motivated the need for biometric quality standardization efforts.
This section, summarizes some of the main issues to be considered regarding the estimation of biometric quality and how it can be used to enhance the performance of biometric systems, giving an overall framework of the challenges involved.

3.1. Biometric sample quality

Biometric sample is of good quality if it is suitable for identification. Recent standardization efforts (ISO/IEC 29794-1) have established three components of biometric-sample quality:

- Character indicates the source's inherent discriminative capability.
- Fidelity is the degree of similarity between the sample and its source, attributable to each step through which the sample is processed.
- Utility is a sample's impact on the biometric system's overall performance, where the concept of sample quality is a scalar quantity that is related monotonically to the performance of the system

In general, in the specialised literature, when speaking about biometric quality experts refer to their *utility* component and it is the case in this study.

3.2. Factors affecting friction ridge image quality

Quality factors may be classified on the basis of their relationship with the system's different parts. We propose to distinguish four classes:

- User-related,
- User-sensor interaction,
- Acquisition sensor,
- Processing-system factors.

Each of these factors is briefly analysed in the following sections.

3.2.1. User related factors

These factors include physical/physiological, as well as behavioural factors. As they are entirely related to the user — a person's inherent features are difficult or impossible to modify — they are the most difficult to control.

Physical /physiological. These include, for instance, age, gender or skin condition — subjects cannot alter the biometric features depending on the biometric system being used. Therefore, recognition algorithms must account for the variability of data in these categories. Also, diseases and injuries can account for feature alterations, sometimes irreversible, possibly making them useless for recognition.

Starting from the full / partial palmprints and fingerprints which are usually of a good quality, these can mostly be attributed to:

- Dry skin
- Excessive sweating
- Elasticity of the skin
- Involuntary damage to the dermal layer (due to illness or occupation – psoriasis, scars, abrasion, etc.)
- Intentional alteration of the fingers (cutting, abrasion, acid)

Skin characteristics. Intrinsic properties of skin vary also depending on the occupation. Skin properties of palms / fingers of a construction worker will not be the same as those of a clerical worker who mostly uses computer in his daily routines. Damage to the dermal layer is observed in some professions – such as for example construction workers or people working with chemicals (acids / bases).

3.2.2. User-sensor interactions fingermarks and palmprints

These factors, which include environmental (room temperature and relative humidity) and operational factors, are easier to control in the case of palmprints and fingerprints than user-related factors, assuming that it is possible to supervise the interaction between the user and the sensor — for example, in controllable premises such as a police station.
In general, these factors also become less relevant as individuals get habituated to use the systems and learn how to interact with them. As in the previous case, the supervision of the acquisition process by a well-trained human operator can reduce, to a large extent, the influence of the following parameters:

- Pressure applied to the sensor is difficult to control. Too much pressure on the sensor results in the introduction of additional (unwanted) artefacts, such as elasticity, distortion, increased thickness of the ridges, while too little pressure usually results in capture of smaller surface of the finger / palmprint.
- Placement, or rather miss-placement, of the finger on the surface of the live-scan device.
- Outdoor use of the fingerprint / palmprint acquisition sensors in "out-of-specification" use-conditions, particularly in dry areas, extremely hot or extremely cold areas may result in enrolment of less-than-usual quality finger / palmprints.

- Feedback to the user regarding the acquired data has been demonstrated to lead to better acquired samples, which can lead to user familiarity with the system.
- Automatic acquisition guidance given by the sensor at the time of acquisition for example providing de user some ques on where to place the face. This can also increase the friendliness of the environment and the overall predisposition of the individual to use it.

The user-sensor interactions are not considered in the case of fingermarks / palmmarks recovered from the crime-scene, as the crime perpetrators do not follow any standards on how to "leave their marks". On contrary, "educated" criminals usually take precautions as to not leave any marks behind. Thus, the crime scene investigators / fingerprint examiners have no control over the dactyloscopic traces recovered. Best practice manuals and laboratory protocols are followed to ensure that the dactyloscopic trace makes it from the crime scene to the forensic laboratory "in the same" condition.

3.2.3. Acquisition sensor factors

The sensor (i.e., live-scan device / scanner) is responsible for reliably translating the physical biometric trait (i.e., subject's fingerprint / palmprint) in the digital domain. Therefore, its fidelity in reproducing the original fingerprint is crucial for the recognition system's accuracy. The diffusion of low-cost sensors and portable devices is rapidly growing in the context of widening access to information and services. This represents an extended scenario for automatic fingerprint recognition systems.
Portable devices usually produce data of inferior quality from that obtained by the sensors used for enrolment of individuals (e.g. booking stations) at the police stations. This is primarily due to their lower sensitivity, worse quality optics and the possibility of user mobility. Additional problems arise when data from different devices coexist in a biometric recognition system—something common in multi-vendor markets. Algorithms must account for data variability in this scenario of sensor interoperability.

3.2.4. Processing system factors

These factors relate to how a biometric sample is processed after it has been acquired. In principle, they are the easiest to control. Constraints on storage or exchange speed might impose data compression techniques — for example in the case of smart cards. Also, governments, regulatory bodies or international standards organizations might specify that biometric data must be kept in raw form (rather than in post-processed templates that might depend on proprietary algorithms), which on one hand may affect size of the data, but on the other hand would support the interoperability.

3.3. Incorporating quality in the friction ridge systems

Quality measurement algorithms are used to modify and improve the processing and final performance of biometric systems in the case of fingerprints and could in principle be used for the same cause in the remaining friction ridge impressions. Such influence in the general work-flow of the system includes:

Quality-based processing. An identification system might apply image enhancement algorithms or invoke different feature extraction algorithms for samples with some discernible quality problem.

- Quality-specific enhancement algorithms.

- Conditional execution of processing chains, including specialized processing for poor-quality data.
- Extraction of features robust to the signal's degradation.
- Extraction of features from useful regions only.
- Ranking of extracted features based on the local regions' quality.

Template updating (updating of the enrolment data and database maintenance). A quality measurement may be used to determine whether a newly-acquired sample should replace the already enrolled sample. Some systems may combine old and new sample features. Quality can be used in both processes.

- Storing multiple samples representing the variability associated with the user (multiple impressions of the same finger).
- Updating the stored samples with better-quality samples captured during system operation.

Quality-based comparison, decision, and fusion. Certain systems may invoke a slower but more powerful comparison algorithm when low-quality samples are compared. Also, the logic that provides acceptance or rejection decisions may depend on the measured quality of the original samples. This might involve changing a verification system's operating threshold for poor quality samples.

Note: The change of the operating threshold (algorithm's sensitivity to the outliers) usually implies changes in the ***expected accuracy*** of the system.

For example, in multimodal biometrics, the relative qualities of samples of the separate modes may be used to augment a fusion process by:

- Using different comparison or fusion algorithms,
- Adjusting those algorithms' sensitivity,
- Quantitative indication of acceptance or rejection reliability,
- Quality-driven selection of data sources to be used for comparison or fusion — for example, weighting schemes for quality-based ranked features or data sources.

Monitoring and reporting across the different parts of the system help to identify problems leading to poor-quality signals and initiate corrective actions. This process can assess signal quality according to these factors:

- *Application*. Different applications might require different scanners, environment set-ups, and so on, which might have different effects on the acquired signals' overall quality.
- *Site or terminal*. Such assessment identifies sites or terminals that pose additional requirements to operator training, operational and environmental conditions etc.
- *Capture device*. Such assessment identifies the impact due to different acquisition principles, mechanical designs etc. It also determines whether a specific live-scan device must be substituted if it doesn't provide signals that satisfy the quality criteria.
- *Subject*. Such assessment identifies interaction learning curves, which can help to better train new users and alleviate the "first-time user" syndrome.
- *Stored template*. Such assessment detects how the database's quality varies when new templates are stored or old ones are updated.

- *Biometric input*. If the system uses multiple biometric traits, such assessment improves how they're combined.

Monitoring and reporting can also support trend analysis by providing statistics from all applications, sites etc. This will let analysts identify trends in signal quality or sudden changes that need further investigation.

3.4. Existing friction ridge quality metrics

Evaluation of fingermark quality begins at the Crime Scene(CS). Trained CS investigators collect the evidence material. Fingermarks found on smaller objects (such as documents, tools, hand-held objects) can be brought to the forensic laboratory for further examination and development, whereas fingermarks found on larger objects (such as wardrobes, door frames, windows) are usually developed / lifted / digitized on-site. It is at the discretion of the CS investigator to determine, which of the fingermarks get collected for analysis.
Typical features the CS examiner looks for in the fingermarks are visibility of ridges, consistency of the ridge-flow, ridge quality, visibility of minutiae, pores, interpapillary ridges, visibility of the patterns and the amount of distortion present in the fingermark. This part of the CS examination process is referred to as evidence pre-assessment.

The fingermarks are forwarded to the forensic laboratory, assigned case numbers and processed by a dedicated fingerprint examiner. Common practice is that one single fingerprint examiner processes all the fingermark evidence from the CS.

While modern AFIS algorithms are capable of operating in "fully-lights-out" mode when searching for an identity of the suspected individual (person) using (normally) a good quality fingerprints (either flat or rolled) in a TP-TP / 1-N comparison, they are not capable of handling CS fingermarks in the same manner. Nevertheless, considering the feedback from the MS, currently some 60% of the cases are handled in the "fully-lights-out" mode with the prospects to treat this way 80-85% of the fingermarks in the near future.

It is known that a fingermark image quality is closely tied to the performance, in particular to the accuracy, of automatic fingerprint comparison algorithms. A good quality fingermark increases the chances of finding the appropriate corresponding fingerprint in a large database as a rank 1 candidate. A dedicated Fingermark and Palmmark Quality assessment algorithm, which is capable of predicting the probative value and accuracy of a comparison algorithm in an automatic way proves useful when pre-processing dactyloscopic evidence.

It needs to be said, that present ABIS fingermark and palmmark recognition algorithms are capable of operating in a fully automatic way without the automatic image quality assessment and quality metric capable of predicting the accuracy of the ABIS algorithm. It is possible due to the fact that the image quality assessment is performed by the dactyloscopic examiners who are trained to assess the probative value of the dactyloscopic trace. However, it needs to be said that although their opinions related to the interpretation of the image quality are based on their experience, they remain subjective.

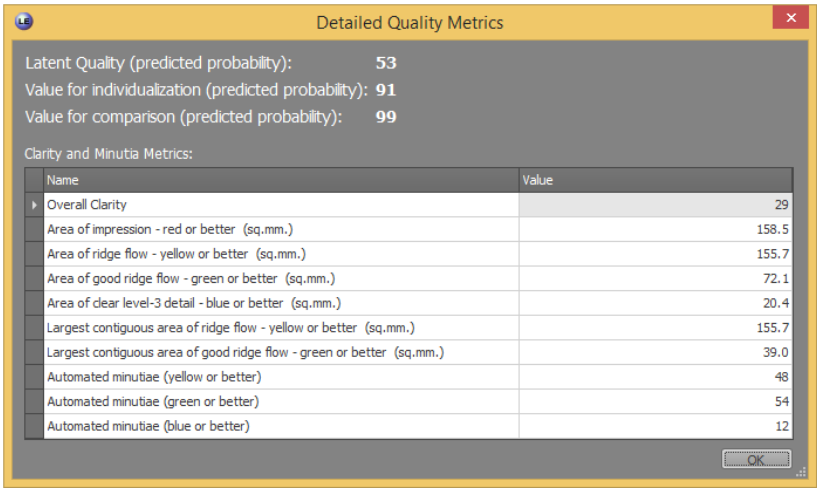
Currently there are several algorithms measuring the quality of fingermarks and predicting the performance of the fingermark comparison algorithms. In order to complete the overview of friction-ridge quality evaluation algorithms, we complement the two above-mentioned fingermark quality evaluation algorithms by the quality algorithms already established in the field of fingerprint recognition, which are due to various reasons (highlighted in the text) less suited for evaluating quality of fingermarks.

3.4.1. LQmetric

Having been primarily developed to support the FBI investigations, the LQmetric has been integrated into the Universal Latent Workstation (ULW) from the version 6.5 onwards [72] [73]. It has been developed in collaboration between the NOBLIS and the FBI. National law enforcement bodies can request a copy of the ULW from the FBI.

LQmetric is an algorithm used for assessment of fingermark image quality based on different factors, such as ridge flow continuity, image clarity, number of minutiae. It supports fingerprint / fingermark / friction ridge images in an FBI default WSQ format in either 500 or 1000ppi resolution. The LQmetric can either be accessed as from the ULW graphical user interface, or as a standalone application using a command line. Both of these provide detailed fingermark image quality metrics (see **Figure 6**).

Figure 6. ULW – detailed fingermark quality metrics (Source: FBI)



When accessed from the GUI, the ULW operator sees the friction ridge image quality on the interface and can decide based on its' "Value for Individualization" (VID) or "Value for Comparison" (VC) whether (or not) to proceed with further processing of the fingermark.
LQmetric can be likewise run from a command line as a standalone application, in which case it returns following components into the selected output directory (depending on the command line options selected):

- LQ score – probability in the {0-100} range. For example, the LQ score equal to 80 for a particular fingermark means that there is 80% probability of retrieving its mate at rank-1.

- VID probability in the {0-100} range – a "crowd-sourced" probability of the fingermark being used by the examiner for individualization in forensic crime investigation context.
- VC in the {0-100} range – a "crowd-sourced" probability of the fingermark being used for individualization or exclusion by a forensic examiner in the forensic crime investigation context.
- Overall image clarity {0-100} – a score (not a probability) is used to assess the quantity of detail in the friction ridge impression.
- Local Clarity map – 125ppi image in the .png format with the input file name as a prefix.
- Minutiae of the automatically extracted from the fingermark in a form of a .csv file.

From the operational point of view (feedback obtained during the visit to the FBI laboratory), the LQmetric integrated into the ULW works well in its task to predict the performance of comparison algorithm for high- and low-quality fingermarks, but not so well on median quality fingermarks – e.g. borderline cases in which the fingerprint examiner hesitates whether a fully automatic fingermark processing is viable.

3.4.2. LFIQ

Determination of fingermark (latent) value was approached by the researchers of the Michigan State University (MSU) as a classification problem [74] [75] [76], in which they assessed whether a fingermark does (VID), or does not have "value" for individualization (non-VID). In their work the feature vectors consisting of varying ridge clarity and minutiae features were evaluated with respect to the resulting accuracy. The results were analysed and showed that the average ridge clarity and the number of minutiae present the two most significant features amongst those studied.
Computation of the local ridge clarity map (RC) consists of several stages, including:

- Pre-processing (contrast enhancement)
- Fourier analysis (decomposition of the image into amplitude, frequency, direction and phase components)
- Ridge continuity map (evaluation of sine waves continuity in two adjacent blocks)
- Final production of ridge clarity map

The minutiae related features considered consist of following:

- Number of minutiae
- Average minutiae quality
- Region of Interest (RoI) – size of the convex hull enclosing the minutiae

The resulting LFIQ measure is defined as a product of average ridge quality and the number of minutiae. With the LFIQ measure defined their next step was to correlate the classification accuracy with the fingermark value. Two types of fingermark value were used:

- Determination by forensic examiners (three labels assigned to each fingermark – VID, VEO, NV, out of which the **VID** class was maintained and the Value for Exclusion Only (VEO) or No Value (NV)were jointly assigned to the class **non-VID**)

- Determination made by the AFIS (two classes were used based on the rank which the corresponding fingerprint was found – **VID** if a match was found on rank < 100 and **non-VID** otherwise)

The overall performance of LFIQ measure based on the minutiae extracted automatically by the AFIS was poorer than that of the LFIQ based on the minutiae marked by fingerprint examiners.

Since the major limitation of the LFIQ was the fact that it relied on manually marked fingermark minutiae (but in principle was capable of handling automatically extracted minutiae), the MSU researchers designed a *FingerMesh* crowdsourcing tool [38] in their subsequent work. They used it for collection of fingermark quality labels from fingerprint examiners and pair-wise comparison quantity labels, determined the underlying bases used by the fingerprint examiners to assign value via MDS and cross-referenced these to the ***automatically*** extracted fingermark features using Lasso. In the last step they "learned" a prediction model for ***automatic*** assignment of quantitative values suitable for ranking an ensemble of questioned fingermarks. Their predicted fingermark value was shown to have high correlation with the performance of a state-of-the-art latent AFIS.

3.4.3. NFIQ

The first version of Fingerprint Image Quality evaluation algorithm was introduced by NIST in 2004 [70]. NFIQ algorithm assigns a discrete predictive quality value (within the 1 : 5 range) to each fingerprint image presented (plain – flat fingerprint), being closely tied to the expected accuracy of a comparison algorithm. The employment of this quality algorithm has been made mandatory in the ANSI NIST ITL 1-2007 standard.
The algorithm behind the NFIQ is relying on a number of known fingerprint quality features, feeding a neural network which was trained on a set of plain (flat) fingerprints with known ground truth. Different file formats of fingerprint images, captured at 500dpi resolution are supported (WSQ, JPEG, NIST IHEAD to name a few). It is therefore not suitable for use on fingermarks, palmprints and palmmarks, and the interested reader is kindly referred to the 2015 version of the JRC technical report [77].

3.4.4. NFIQ2

The process of upgrading the NFIQ to NFIQ2 [78] was initiated 2011 as a joint project between the NIST, Federal Office for Information Security (BSI), the Federal Criminal Police Office (BKA) in Germany and research institutes MITRE, Fraunhofer IGD, Hochschule Darmstadt and Secunet [79].

The NFIQ2 algorithm extracts fingerprint features, which is fed into a random forest (RF) machine learning algorithm. It outputs fingerprint quality scores in the 0-100 range in compliance with the ISO/IEC 29794-1:2016[37] standard. Upgrades comparing to original NFIQ include: "*lower computation complexity and support for quality assessment in*

[37] ISO/IEC 29794-1:2016 – Information Technology :: Biometric Quality :: Part 1 Framework

mobile platform"[38]. NFIQ2 features are being formally standardized as a part of the ISO/IEC 29794-4[39] standard.

NFIQ2 was pretrained on a set of "flat" fingerprint images to produce the fingerprint quality score. As in the case of NFIQ, the NFIQ2 algorithm has been optimized for 500dpi resolution RAW or WSQ fingerprint images (live-scan or inked). It is therefore primarily not designed to work on fingermarks, palmmarks or palmprints and interested reader is referred to the 2015 version of the JRC technical report [77].

The NFIQ2 algorithm is available as an open-source and in principle it should be possible to re-train the algorithm on the fingermark images, thus adapting it to output quality metric for fingermarks, palmmarks and palmprints.
The added value of this approach is somewhat questionable, as the standard fingerprint features usually don't contain texture information which is extracted from the fingermark images.

3.4.5. DCT based quality metric for 10-print cards

Latest research conducted by the Institute of Forensic Science Ministry and Public Security in China [80] led to development of new multi-stage method for evaluation of fingerprint image quality based on two-dimensional weighted Discrete Cosine Transform (DCT) block. The method was developed to work with live-scan fingerprint images. In the first stage they check for grey inversion in the scanned image, in second stage they project the fingerprint image *"in a horizontal direction"* and evaluate the distance between the core of the fingerprint and centre of the image. Third stage is reserved to two-dimensional DCT transform, which is used to evaluate the sharpness of the image.
Although the authors suggest that their method is *"effective and feasible"*, it is not clear how many fingerprints the method was trained or evaluated on. This potentially promising research could benefit from thorough evaluation on existing datasets (e.g. NIST SD4, SD27) and put in contrast with the NIST NFIQ2 quality metric. It is also unclear, whether their same method could be adapted for the use on partial fingerprints, fingermarks or palmmarks.

3.4.6. Palmprint quality metric

Palmprint quality assessment and evaluation is by many considered a necessary pre-requisite for successful identification in 1:N comparison. Different friction ridge quality metrics have been developed in the past. Depending on the scenario used, there are the NIST quality metrics for assessment of quality of fingerprints (NFIQ, succeeded by NFIQ2), MSU's LFIQ for assessment of fingermark image quality, as well as the FBI's LQmetric (a fingermark quality assessment tool integrated in the latest versions of their Universal Latent Workstations).
The Ridge-Based Forensic Palmprint Image Quality Measurement (RFPIQM) was recently proposed by the research team from the Shandong Jianzhu University in China [81]. In their work they propose to measure image quality of a partial or full palmprint from a forensic database based on the ridge properties. First, two new features (ridge period

[38] https://www.nist.gov/sites/default/files/documents/2016/12/07/nfiq2_report.pdf

[39] ISO/IEC 29794-4:2016 – Information Technology :: Biometric Quality :: Part 4 Finger Image Data

and ridge orientation variance) are introduced to assess the palmprint image quality and combined with ridge orientation continuity, ridge thickness uniformity and ridge valley contrast to enhance the classification performance.

The image quality assessment method proposed is a multi-stage process. First the local block-wise image quality measurement, in which a local quality model produces the local quality labels. These enter into the global full palmprint image quality measurement, together with the global information, to produce global features which enter into the multi-classifier training stage. The global quality prediction occurs in the last stage, which uses the input from the multi-classifier training and the global information from the queried image to produce the ***global quality label***.

In order to obtain the quality labels using the four classification algorithms, authors have manually assigned quality classes to blocks (5 quality classes), as well as to the full palmprints (3 quality classes).
The block approach (partial palmprint image quality assessment algorithm) in this work was treated as a binary or a multiclass (3 and 4 classes) supervised learning classification problem, which aims to distinguish between the manually assigned labels of good quality. Results are reported for all classification problems. Overall, the block approach of RFPIQM resembles the first version of NIST NFIQ algorithm although, it is not clear why results on the multiclass (5 classes) classification problem, based on 5 manually assigned quality classes, were not reported.

Full palmprint image quality was treated as a binary or a multiclass (3 classes) supervised learning classification problem, aiming to distinguish between a good/bad quality labelled palmprints or amongst all three classes.
All the results reported in this work are based on full / partial high resolution palmprints. The RFPIQM produced a global quality map for each queried palmprint (equivalent to quality map produced by the LQmetric) and should, according to the authors, work with the palmmarks, as long as they are "not too small". An equivalent study is therefore necessary to assess the performance of the RFPIQM on palmmarks.

Overall, this work can be seen as an excellent starting point, which could be further extended to provide either a single numerical value output on a discrete scale (equivalent to the NFIQ) or a single numerical value output on a continuous scale in a 0-100 range (equivalent to NFIQ2 and LQmetric).

Section 3. Summary of key concepts

- Assessment of quality of the friction-ridge impressions is important, as higher quality samples tend to produce comparison scores of higher magnitudes. It also tends to be easier (also for human examiners) to extract reliable features from good quality friction ridge impressions.

- Unlike the fingerprints, where the NIST developed NFIQ2 was embraced by a forensic scientific community and police laboratories and is being used as a "de-facto" standard alongside the proprietary metrics of different technology providers, a similarly reliable open-source metric is currently not available for the remaining friction ridge impressions.

- NFIQ2 fingerprint quality metrics cannot be used with fingermarks and palmmarks as this algorithm has been trained with flat fingerprints only.

- Some shortfalls have been reported using the ULW's LQmetrics – while it works reliably for good and bad quality fingermarks, it struggles in the "grey areas" where even the fingerprint examiners find it difficult to attribute a value for comparison (VC).

- The efforts of the MSU researchers summarized in their publications on the LFIQ could lead to a possible NFIQ2 equivalent for fingermarks, providing that their application would made available to the fingerprint community and adopted by the fingerprint community (optionally standardized).

- The palmprint quality metric (RFPIQM) presented in the section 3.4.6 demonstrates the recent efforts on the complex issue of palmprint quality assessment. Although comparable to the original NFIQ, it is not a "ready-to-use" open-source product which would be available to the forensic community.

- Further effort in terms of time and resources should be dedicated to the development of an image quality metric for fingermarks and palmmarks.

4. Standards applicable in friction-ridge biometrics

Biometric data interchange standards are needed to allow the recipient of a data record to successfully process data from an arbitrary producer. In other words, biometric interoperability means that biometric data, in whatever form (i.e., raw samples, templates, scores) can be accurately exchanged and interpreted by different applications. This can only be achieved if the data record is both syntactically and semantically in compliance with a published standard.

Following advances in biometric technologies as a reliable identity authentication technique, more large-scale deployments (e.g. e-passport) involving multiple organizations and suppliers are being rolled out. Therefore, in response to a need for interoperability, biometric standards have been developed.

Without interoperable biometric data standards, exchange of biometric data among different applications coming from different vendors is not possible. Seamless data sharing is essential to identity management applications when enrolment, capture, searching and screening are done by different agencies, at different times, using different equipment in different environments and/or locations. Interoperability allows modular integration of products without compromising architectural scope, and facilitates the upgrade process and thereby mitigates risk of obsolescence.

Table 4 lists the main standards organizations and other bodies working on the development of biometric standards. Current development focuses on acquisition practices, sensor specifications, data formats, technical interfaces and extended feature sets. The two main entities working in biometrics standards are the ISO/IEC JTC 1/SC 37 and the ANSI/NIST[40].

Table 4. Main organizations working on the development of Biometric standards

Biometric standard organizations
International Standards Organizations:
IEC: International Electrotechnical Commission (www.iec.ch)
ISO-JTC1/SC37: International Organization for Standardization, Committee 1 on Information Technology, Subcommittee 37 for Biometrics (www.iso.org/iso/jtc1_sc37_home)
CEN: European Committee for Standardization (www.cen.eu)
National standards bodies:
ANSI: American National Standards Institute (www.ansi.org)
Standards-developing organizations:
ICAO: International Civil Aviation Organization (www.icao.int)
INCITS M1: International Committee for Information Technology Standards, Technical Committee M1 on Biometrics (http://standards.incits.org/a/public/group/m1)
ANSI/NIST-ITL: American National Institute of Standards and Technology, Information Technology Laboratory (www.nist.gov/itl)

[40] A registry of US government recommended biometric standards (www.biometrics.gov/standards) offers high-level guidance for their implementation.

International institutions active in the research and development in the area of forensic biometrics, participating to the development of best-practice manuals and guidelines are listed in **Table 5**. Both tables are populated to the best knowledge of the authors, it may however not be completely exhaustive.

Table 5. Organizations active in development of biometric guidelines and best-practice manuals

Other organizations
BC: Biometric Consortium (www.biometrics.org)
BCOE: Biometric Center of Excellence (www.biometriccoe.gov)
BIMA: Biometrics Identity Management Agency (www.biometrics.dod.mil)
IBG: International Biometric Group (www.ibgweb.com)
IBIA: International Biometrics and Identification Association (www.ibia.org)
ENFSI: European Network of Forensic Science Institutes (enfsi.eu)
EAB: European Association for Biometrics (www.eab.org)

4.1. Most relevant fingermark / palmmark standards

Concerning the specific exchange of biometric data, the most relevant standards are:

- ISO/IEC 19784-1:2006 BioAPI 2.0
- ISO/IEC 19785-1:2015 Common biometric Exchange Formats Framework
- ISO/IEC 19794-4:2011 Biometric data interchange formats – Finger image data
- ISO/IEC 19794-2:2011 Biometric data interchange formats – Finger minutiae data
- ANSI/NIST ITL 1-2011 Update 2015. Data format for the interchange of fingerprint, facial and other biometric information.
- CJIS-FBI EBTS v10.0.8:2017 Electronic Biometric Transmission Specification
- ISO/IEC 19795: Information technology – Biometric performance testing and reporting
- ISO/IEC TR 29189: Information technology – Biometrics – Evaluation of examiner assisted biometric applications
- ISO/IEC 39794-1:2019 Extensible biometric data interchange formats – Framework
- ISO/IEC 39794-4:2019 Extensible biometric data interchange formats – Fingerprint image data

Although the ICAO standard describes the use of fingerprints (thus is friction-ridge related), it is mostly dedicated to usage and storing of live-scanned fingerprints and does not consider fingermarks, full or partial palmprints or palmmarks. Therefore, it will be omitted from this review.

4.2. ISO/IEC 19784-1:2006 (BIOAPI 2.0)

ISO/IEC 19784-1:2006 provides a defined interface that allows a software application to communicate with (utilize the service of) one or more biometric technologies. It includes a high-level generic biometric authentication model suited to a broad range of

biometrically enabled applications and to most forms of biometric technology. An architectural model is defined, which allows the biometric system components to be provided by different vendors, and to interwork through fully-defined Application Programming Interfaces (APIs), corresponding Service Provider Interfaces (SPIs), and associated data structures. This standard covers the basic biometric functions of enrolment, verification and identification, and includes a database interface that allow an application to manage the storage of biometric records. Conformance requirements are identified and informative annexes, including sample code, are provided. ISO/IEC 19784-1:2006 specifies a biometric data structure which is compatible with ISO/IEC 19785 and 19794.

4.3. ISO/IEC 19785-1:2015 Common Biometric Exchange Formats Framework (CBEFF)

This standard defines structures and data elements for Biometric Information Records (BIRs). It defines also the concept of a domain of use, to establish the applicability of a standard or specification that complies with CBEFF requirements. It defines the concept of a CBEFF patron format, which is a published BIR format specification that complies with CBEFF requirements, specified by a CBEFF patron. Likewise defined are the abstract values (and associated semantics) for a set of CBEFF data elements to be used in the definition of CBEFF patron formats. It specifies the use of CBEFF data elements by a CBEFF patron to define the content and encoding of a Standard Biometric Header (SBH) to be included in a biometric information record.
The ISO/IEC 19785-1:2015 provides the means for identification of the format of the Biometric Data Blocks (BDBs) in a BIR but the standardization and interoperability of BDB formats are not in the scope of this part of the standard. It also provides a means (the security block) for BIRs to carry information about the encryption of a BDB in the BIR and about integrity mechanisms applied to the BIR as a whole; the structure and content of security blocks are not in the scope of this part of the standard, as well as the specification of encryption and integrity mechanisms for BIRs.
This standard specifies transformations form one of CBEFF patron format to a different CBEFF patron format. The encoding of the abstract values of CBEFF data elements to be used in the specification of CBEFF patron formats is not in the scope of this part of standard. It also specifies several security block format specifications for which ISO/IEC JTC 1 SC 37 is the CBEFF patron.
Protection of privacy of individuals from inappropriate dissemination and use of biometric data is not in the scope of this part of ISO/IEC 19785 but may be subject to national regulation.

4.4. ISO/IEC 19794-4:2011 Biometric data interchange format – Finger image data

This biometric standard defines the biometric fingerprint interchange format for storing, recording and transmitting fingerprint or palmprint information in the previously introduced ISO/IEC 19785-1 data structure. The format can be used for transmission and comparison of friction-ridge image data. It includes the content, format, and units of measurement for finger image data exchange which may be used for identification (1:N comparison) or verification of identity (1:1 comparison) of the individual. For this purpose, various mandatory and optional elements are defined, for example the compression of digital images, scanning or vendor-specific parameters. The information

within standard is intended to support the inter-organization exchange of friction-ridge data, which can be used by ABIS. Information compliant with ISO/IEC 19794-4:2011 can be recorded on machine-readable media or may be transmitted by data communication facilities.

4.5. ISO/IEC 19794-2:2011 Biometric data interchange format – Finger minutiae data

The finger minutia data part of the ISO 19794 biometric standard defines the concept and data formats for minutiae encoding in a generic way so, that it can be used in a range of ABIS scenarios.
It contains information on how minutiae are to be marked, storage data formats for general use and use with e.g. 10-print cards and information on conformance.
Within this standard, following elements are specified[41]:

- "the fundamental data elements used for minutiae-based representation of a fingerprint;
- three data formats for interchange and storage of this data: a record-based format, and normal and compact formats for use on a smart card in a match-on-card application;
- optional extended data formats for including additional data such as ridge counts and core and delta location."

4.6. ANSI/NIST-ITL 1-2011 Update:2015

In 2015 NIST has published an update on the American National Standard for Information Systems ***ANSI/NIST-ITL 1-2011***[42] related to "Data Format for the Interchange of Fingerprint, Facial and Other biometric information. From this standard the NIST container used for exchange of biometric data in SIS is derived.

Amongst many different types of (not only) biometric data specified in this standard, following types are the most relevant for this report:

- Type 13 Fingermark or Palmmark image (partial friction ridge impression usually lifted at the crime-scene)
- Type 14 Fingerprint 10-print record
- Type 15 Palmprint record
- Type 9 Minutiae data and Extended Feature Set (EFS)

The optional EFS part of the type-9 minutiae set contains additional information, which can be used by ABIS systems to boost the performance of comparison algorithms. It can contain following information: Origin of Friction Ridge (Palm/Finger/Foot), Region of Interest (ROI), Angles and Orientation of the fingermark / palmmark, Position, Feature set profile, Pattern Classification, Ridge Quality Map, Ridge Flow Map, Ridge Wavelength map, Quality of the Palmmark / Fingermark, Indication of Growth / Shrinkage, Deltas / Cores (or indication of them missing), Core-Delta Ridge Counts, Centre Point of

[41] Source : ISO/IEC19794-2:2011 Information technology,-- Biometric data interchange formats – Part 2: Finger minutiae data

[42] ANSI/NIST-ITL 1-2011 Update:2015 http://dx.doi.org/10.6028/NIST.SP.500-290e3

Reference, Distinctive Features, EFS minutiae, EFS Minutiae Ridge Counts, Pores, Creases, EFS Method Detection and other.

4.7. EBTS v10.0.8:2017

With the aim to move towards a system capable of containing a complete set of biometric and biographic information of a subject in their databases, the Criminal Justice Information Services (CJIS) division of the FBI published new version of the Electronic Biometric Transmission Specification (EBTS) standard in September 2017. This standard has been developed for electronic encoding and transmission of biometric data as an ANSI/NIST-ITL standard profile. Requirements for logical records set forward in the ANSI/NIST-ITL are maintained in the EBTS. Although FBI's primary biometric characteristic used to identify individuals remains a fingerprint record, this version of EBTS contains additional biometric characteristics – facial image, iris, palmprint.
While the ANSI/NIST-ITL standard defines the communication and interchange of biometric data between the agencies, the EBTS lays forward the requirements with which the agencies must comply when communicating with the FBI.

4.8. ISO/IEC 19795: Information technology – Biometric performance testing and reporting

This ISO/IEC 19795 standard contains multiple parts relevant for the testing and reporting of biometric systems used (not only) in forensic biometrics. Performance metrics for different interactions with the biometric systems for the enrolment, verification and identification scenarios, are unambiguously defined. Some of these performance metrics are used (and will be referred to) in the performance evaluation part of this report.
Three different types of biometric performance testing are considered – technology, scenario and operational evaluation. Different protocols and procedures are used in each type and produce different results. The standard is split into the following main parts:

- Part 1: Principles and framework
- Part 2: Testing methodologies for technology and scenario evaluation
- Part 3: Modality specific testing [Technical report]
- Part 4: Interoperability performance testing
- Part 5: Access control scenario and grading scheme
- Part 6: Testing methodologies for operational evaluation
- Part 7: Testing of on-card biometric comparison algorithms

Although some parts of this standard are of particular interest for the report, it is beyond its scope to describe the different technical aspects of this standard in more detail. The interested reader is therefore kindly referred to the ISO online library[43].

[43] https://www.iso.org/standard/41447.html

4.9. ISO/IEC TR 29189: Information technology – Biometrics – Evaluation of examiner assisted biometric applications

This technical report addresses the human assisted biometric applications particularly in scenarios, in which the quality of biometric samples can be degraded due to various factors to a point at which the biometric sample is no longer suited for automated processing and human input is required. It is the case for example in fingermark comparison, where a fingerprint examiner may intervene in the process of sample capture, enrolment, template generation and interpretation of comparison scores.
If the human examiners interact with an automated biometric system at any of the above-mentioned stages, such a system is deemed "examiner assisted" and its benefit is twofold – they *"assist the human examiner to perform their role more effectively"* and *"allow the expertise of human examiner to be exploited to assist the automated comparison process"*.
The main benefit of such systems is in "offline" scenarios, in which the immediate response of the biometric system is not required. According to the technical report, the role of the examiner *"…is crucial, as it impacts on the design of the system, the manner in which it is used, how it is tested, and how the system performance and its individual subcomponents are defined and measured."*
In the scope of the technical report presented in this technical report, the assessment of biometric system is considered *"either as whole, or by testing the examiner assisted and automated elements separately."*

Although this technical report deals with the evaluation of examiner assisted applications and is very relevant for processing fingermarks and palmmarks, it has no immediate implications on the CS-SIS, as no human intervention is foreseen on the dactyloscopic traces from the moment they are introduced in the CS-SIS in the form of an alert. All the aspects related to human intervention, including the comparison scores evaluation will be performed outside of CS-SIS, on the premises of MS in accordance with their respective national laws.

4.10. ISO/IEC 39794-1,4:2019 Extensible biometric data interchange formats – Framework and Fingerprint Image data

The SC37 committee of ISO/IEC standardization body is currently working on a new standard of extensible biometric data interchange formats, which will eventually supersede the previous two standards (ISO/IEC 19794-2 and ISO/IEC 19785-1). Both parts 1 (Framework) and part 4 (finger image data) are currently under development and are expected to be published by the end of 2019. This will be, at the time of publishing, one of the most advanced and up-to-date standards in biometric technology particularly in the field of biometric fingerprint recognition.
Its most relevant and innovative feature with respect to previous standards is that it is "extensible", meaning that it is not only backward compatible with previous standards, but also forward compatible so that new features (e.g. EFS) can be added to the data containers in order to keep up with the rapid advances witnessed nowadays in the field of biometric technology.

Section 4. Summary of the key concepts

- Standards are determinant elements in order to ensure the interoperability and interchange of data between end-users, as well as between different National and EU large-scale IT systems. It is particularly relevant in cases when the enrolment and subsequent searches are performed by different national authorities using systems provided by different vendors / different versions of the systems.

- Standards, and in particular definitions contained within contribute to specify in a clear and non-ambiguous way the operational requirements, implementation procedures, measures of performance and many other important elements contributing to a high level of accuracy.

- Most relevant and most widely used standards are those of ISO/IEC and ANSI/NIST.

5. Part I. Lessons Learned: Challenges faced by ABIS-Fingermark, Palmmark and Palmprint technology

5.1. Fingermarks:

Crime-scene recovered fingermarks and palmmarks of unknown individuals in the scope of criminal are processed in every country / agency visited. Different practices, sometimes even within the same dactyloscopic department were observed at the level of processing of crime-scene recovered traces. The fingermarks / palmmarks are recorded at 1000dpi or 500dpi resolution. If a national AFIS operates with 500dpi images, the 1000dpi fingermarks are downsized for the purpose of comparison, however if available, a high resolution fingermark / palmmark image is stored in the Unsolved Latent Files(ULF) dataset.

Once the fingermark / palmmark is digitized, (this process is not necessarily performed by a dactyloscopic expert but may be substituted by a trained staff at the crime-scene laboratory), the digital impression is *analysed* by a skilled dactyloscopic examiner.

Several years of training on high quality fingerprints followed by an exam are a common pre-requisite for dactyloscopic examiners to move to evaluation of fingermarks / palmmarks which are rightly considered as more challenging. Fingerprint examiner proceeds with the mark-up of the fingermark in order to determine the value of the fingermark – VID, VEO, NV (see section 3.1). This can be achieved by:

- Manual feature extraction and manual comparison
- Supervised semi-automatic feature extraction (lights-out feature extraction by the ABIS followed by human verification)
- Fully-lights-out automatic feature extraction with no human intervention

Several factors influence the choice of the level of intervention on the fingermark / palmmark, such as image quality, ridge clarity, orientation of the fingermark, presence of core / delta, etc.

Although numerical standards exist in majority of the countries visited, these are only followed for identification of the individual in legal context. Fingermarks / palmmarks showing number of minutiae inferior to the numerical standard still present a potentially valuable input and are used as "investigative leads".
In order for a fingermark / palmmark to be ***searchable*** by ABIS (able to produce a searchable template), some manufacturers recommend that "minimum number of minutiae" should be present (quoting the manufacturers, this number should be at least 3).

Note: "ABIS-searchable" biometric template does not mean that the fingermark will be "***claimable***" in the judiciary process of any given MS.

Common denominator is the ***subjective determination*** of quality of fingermark / palmmark images by fingerprint examiners. Fingerprint practitioners in all countries visited highlighted the need for the development of reliable fingermark / palmmark quality metric, which would help to predict the performance of the comparison algorithms.

Some MSs reported experimenting with vendor proprietary Fingerprint Image Quality (FIQ) metrics. Other experiment the use of NFIQ2 for fingermark quality evaluation[44].

National AFIS systems are supplied by different manufacturers and the features (minutiae coordinates and extended feature sets) encoded on local NS-AFIS may not necessarily correspond to the features which might be used / extracted by the CS-SIS fingermark ABIS. Several options are highlighted in section 9 - Interoperability.

Fingermarks deemed having Value for Comparison (VC) are submitted to the national AFIS for automatic comparison. There are several modes of interaction with the national AFIS and the operator may choose from submitting:

- only image (assuming sufficient quality for fully lights-out search)
- image and marked ROI (assuming sufficient quality for fully lights-out search)
- image, marked ROI and minutiae points (automatic, semi-automatic or manual mark-up)
- image, marked ROI, minutiae points and extended feature set (EFS compatible with NS-AFIS)

The ABIS fingermark system is not equivalent to the HIT / NO-HIT system operating at a certain threshold like fingerprints (which also returns a rank-list of candidates). A search with fingermarks, palmmarks returns a rank-list of candidates which is subjected to further analysis by dactyloscopic experts.
The size of rank-lists differs amongst the national authorities. They typically also differ internally depending on the severity of the crime. In cases of serious crimes or suspected terrorist activity the rank list can be as long as 200 candidates.

It is reasonable to assume similar mode of interaction in the future between the MS and CS-SIS. Therefore, operator interacting with CS-SIS should be "*ready to invest resources*" into the verification of potential matches on the side of MS.

If the fingermark is not matched, the operator has the choice of storing it in the database of Unsolved Latent Files (ULF). This database is shared by logically separated fingermarks and palmmarks. Bad quality fingermarks / palmmarks (not possible to search by national AFIS) originating at a scene of serious crime / terrorist activity can be stored as "image only". A match on an ULF database is verified by multiple examiners. Depending on the severity of the crime up to 7 different examiners can be involved in some agencies.

It is a common practice in majority of countries visited to search the fingerprints / palmprints of a new person, booked at the police station, against the ULF. Skilled fingerprint examiner can infer the "MATCH / NO-MATCH" result from the relative distance between the comparison scores returned with the rank-list of candidates. An example could be a relative distance between the rank-1 score and the scores of nearest cohort (e.g. ranks 2-5).

[44] It should be noted, that NFIQ2 has been developped, tested and evaluated on flat fingerprint images and not on the fingermarks/palmmarks.

In order to reduce contextual, some MSs experiment with the ways ranked lists of candidates produced by the AFIS algorithm are presented to the examiners for subsequent analysis:

- return a rank list of candidates with accompanying comparison scores
- return a rank list of candidates with no comparison scores
- return a rank shuffled list of candidates

Although this approach may lead to somewhat "more objective evaluation of the fingermark evidence" (it forces the fingerprint examiner to consider the entire list of candidates), the differences in the magnitude of comparison scores of the nearest cohort (for example first 5 candidates), provide priceless inference tool particularly in times of significant workload.

Slight difference is reported by the vendors in terms of processing speed for comparing individual fingermarks / palmmarks and comparing full fingerprints. The process which is "***more time consuming***" is the feature extraction, as the fingermark / palmmark comparison usually relies on the "extended feature set". Nevertheless, 15s turn-over of (up to) 4 fingerprints captured at the border can be assumed for border **4P → LP** border application.

Although technically possible, fingermark to ULF **LP → LP** comparison is very rarely used amongst the authorities visited as it is technically the most challenging use-case. Typical reasons include (but are not limited to) degraded quality; small (partial) surface; small number of minutiae; with it linked low probability of producing two fingermarks of the same finger showing at least some features in correspondence; and human resources needed to verify the candidate lists.

5.2. Palmmarks:

Some statistics obtained in the US show, that approximately 30% of the dactyloscopic traces lifted at the crime-scenes are account for palmmarks [52]. Therefore, palmmark to full palmprint comparison can be clearly relevant.

It is unclear if similar numbers can be expected in the EU, as the availability of the palmprints and palmprint databases varies greatly across the MS. It should be mentioned that the palmprints are in general less studied than the fingerprints.

As explained in section 2.2, the ROI of palmprints is significantly larger comparing to the fingerprints. In other words, comparing full palmprints requires a lot more resources in terms of computing power and time. Normally, full palmprints are collected together with a full set of fingerprints – rolled and flat – which are preferred means of identification amongst the agencies.
Thus, although technically feasible using existing technology (current AFIS systems), full-to-full palmprint comparison is rarely used.

Considering the feedback from the technology vendors, according to their internal tests (as no palmprint recognition vendor test was organized to date and there is limited access to palmprint datasets), the palmprint comparison is deemed as accurate as fingerprint comparison, in some cases better as more features (minutiae) are present in a typical palmprint. Nevertheless, the sizes of the respective datasets for palmprints and

fingerprints appear not to have been taken into consideration when making those statements.

Section 5. Summary Lessons Learnt

All the information regarding automatic fingermark and automatic palmmark identification technology gathered during the review of the state of the art and during the visits to the MSs, has allowed us to identify the main challenges currently faced by this type of technology. Such challenges, which in many cases are interlinked, can be summarized as follows:

Use-cases: probably the most critical parameter, which contains scenarios and operational context in which the systems will be used. These use-cases will determine, to a large extent, the type and number of transactions (enrolment and consultations) that the system will have to handle. The remaining parameters listed below are related to this one.

Performance: the accuracy of the ABIS system and its ability to correctly attribute a queried identity in a given database. Very high accuracy is crucial particularly when system in place has to interact with large database.

Quality: biometric sample quality of the fingermark / palmmark images which are stored / searched in the system. Maintaining a high quality of the biometric samples, particularly those enrolled in the database, is critical to achieve a desired high level of accuracy.

Integrity of the database: refers to the correctness of the data stored in the ABIS database. Typical errors that are usually observed in ABIS databases include: wrongly assigned finger number (if known), misclassification of first level features (general patterns – although this feature is being less used nowadays), inconsistency between the alphanumeric description of the fingermark and the fingermark image in the sample record, missing fingermark image.
In case of palmprints these can be wrongly assigned palmprint image (left or right hand), palmprint images not corresponding to the right identity, missing palmprints, inconsistency between alphanumeric data and palmprint data, multiple entries of the same palm with multiple identities (multi-alias) etc. It is critical for the correct functioning of ABIS-Fingermark, Palmmark and Palmprint systems to mitigate, as much as possible, this risk.

Type of data being processed: with regard to the use-cases, it is important to define the type of Fingermark and Palmmark images that the system will have to work with at all levels – enrolment, consultation and test. Full palmprints contain a lot more information than fingerprints, though the quality / surface captured varies when different methods are used – inked – flat, inked – rolled, live-scan flat. The quality of the different type of data types differs significantly and was proven to have an impact on the accuracy and comparison capabilities of the ABIS.

Searchable Fingermarks / Palmmarks: these pose a significant challenge for the ABIS systems. The key question from the automatic comparison point of view is: "are there enough features present in the image for a feature extraction algorithm to function properly"? Not enough features in a fingermark / palmmark image submitted to an ABIS system can result either in "not suitable for comparison" error or in a rank list of candidates for which all of the comparison scores will be at the level of background noise.

Speed: in other words, the response time of the system when a query (i.e. consultation) is launched. The response is a critical parameter for some use-cases, in which the time constraints are very strict (e.g., first line of check border control). The response time is different when comparing fingerprints in TP → TP transaction, much higher in a PP → PP transaction and different in LP → TP or LP → PP transaction.

Size of the database: or the number of unique identities enrolled in the system database with which the comparison algorithms interact. This parameter is one of the key design features and should be carefully considered prior to integrating any ABIS system into SIS. The size of the database will have a big impact on the response time of the system and is one of the features to be considered when defining the minimum accuracy expected for the system. It will also have impact on the False Positive Identification Rate.

Number of transactions at peak hours: together with the database size and the expected response time, this feature is also a key design feature to size of the ABIS (in terms of the necessary processing power). It refers to the capacity of the ABIS to handle consultations and should be taken into consideration and carefully estimated in the design phase.

Comparison capacity: refers to the maximum number of transactions (i.e. comparisons between individual fingermark / palmmark samples) that the system is able to perform at peak hours. This parameter may vary depending on the type of transaction and the use-case.

Strategy to handle the queries: although this may be considered a secondary feature it may play a very important role in the transaction response time and therefore in the resources needed by the ABIS Fingermark / Palmmark. Depending on the use-case, it can be useful to assign a priority to each type of transaction, depending for instance on the expected response time.

Exchange formats: it is essential to define a unique, standardized exchange format for the different type of data handled by the system (e.g. fingermark images, fingermark templates, minutiae, quality scores, etc.). It is particularly important to well define the extended feature set (EFS) interchange format for Fingermarks and Palmmarks, as these have proven to boost the performance of ABIS system used. The accuracy and reliability of EFS generated by different algorithms should also be tested and evaluated on real operational ground-truth datasets.

Multiple records: the possibility to store multiple palmmark / fingermark records offers opportunity to use "search the highest quality record" strategy. The strategy may vary according to the type of record submitted for consultation (fingermark / palmmark / palmprint).

Operational procedures: operational procedures in the way ABIS fingermark operators interact with their systems vary (e.g., fingermark / palmmark enrolment methodology). On the other hand, manual annotation, fully lights-out annotation or semi-automatic annotation of fingermarks and palmmarks has been reported by the MSs (in some cases all three approaches allowed within one unit). Difference in the approaches may have an impact on the overall accuracy of the system. Therefore, harmonization of these methodologies and the best practices should be envisaged in order to achieve the maximum possible accuracy of the system.

Human intervention: is closely linked to the previous point, where in some cases manual annotation or semi-automatic approach, in which the fingermarks / palmmarks are processed automatically and human operator intervenes on the automatically detected features (marking the ROI, removal of minutiae at the periphery of the image, etc.). The human intervention in this case presents additional "quality-assuring" element.

Maintenance and performance evaluation: benchmarking the accuracy of an ABIS system is a mandatory task to be conducted during the life-cycle of a biometric system. As mentioned above, there are several different elements which affect the accuracy of ABIS (size of database, quality of biometric samples, etc.). Another crucial aspect is that the ABIS systems integrated into the SIS are not "the ultimate versions" and are subject to contractual maintenance and upgrades. Common best practice amongst the MSs is the benchmark of their national ABIS system at least with every new version of ABIS deployed.
Thus, this task not only provides important information on the accuracy of the system in production (with real data) but can also be a useful tool for fine-tuning the system and eventually improving its performance.

System architecture: all the previous technical features, as well as other parameters derived from the specific context in which an ABIS fingermark and palmmark will be deployed, should be considered during the design phase in order to select the most suitable architecture (e.g. distributed, centralized, hybrid).

The aim of the next part of the report will be to detail and address these challenges, whenever possible, in the context of SIS and its potential ABIS Face functionality.

Part II
Overview of CS-SIS

PART II of this report is focused on CS-SIS and its future ABIS Fingermark and Palmmark functionality. This part refers to and builds upon many of the concepts, terms and general aspects described in PART I. PART II is based on the following rationale:

First, considering its legislative framework, a description of the key aspects concerning CS-SIS today is presented.

Second, according to the newly adopted legislation last November 2018, we present the main upgrades that should be performed in CS-SIS in order to integrate the new functionalities defined.

Third, according to the challenges exposed in section 5 (PART I) and to the specificities of the SIS described below in section 7 (PART II), a series of recommendations are presented on how to address these challenges in order to implement an ABIS Fingermark and Palmmark in CS-SIS in the most effective and successful manner.

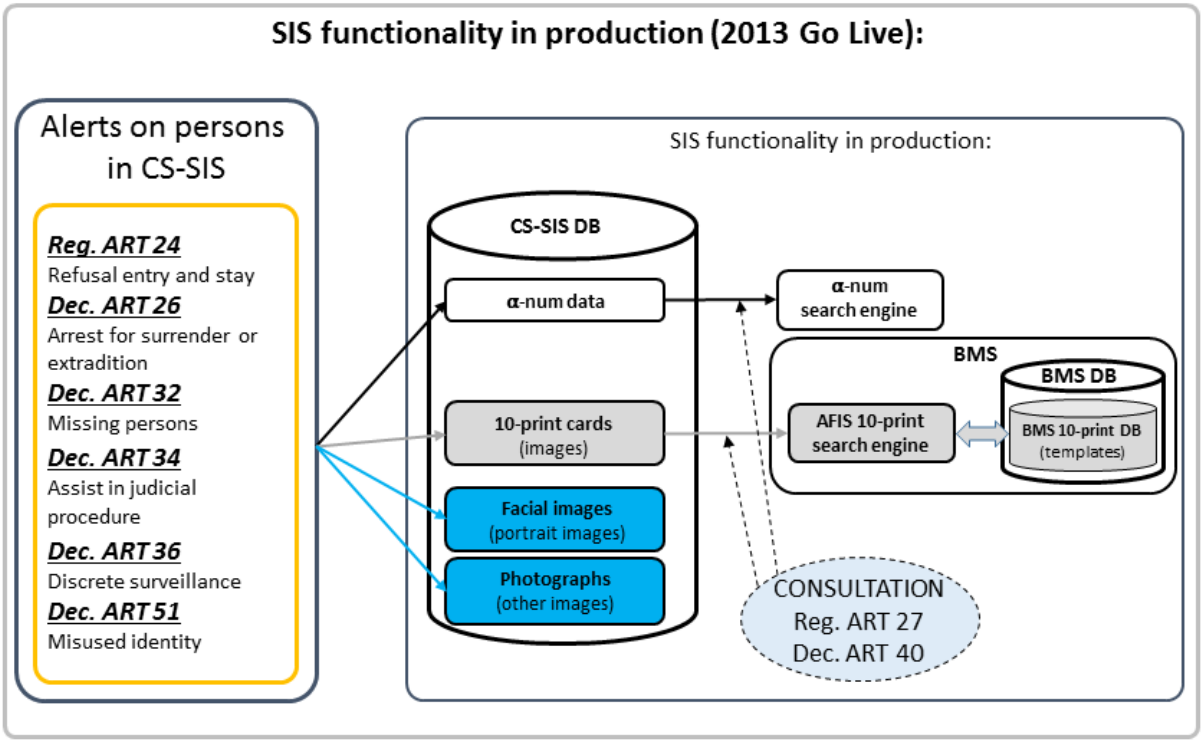
Fourth, taking into consideration trends set out by the latest advances in the Fingermark / Palmmark recognition technology we look beyond today's regulatory framework, and describe possible future functionalities that could further enhance the capabilities of CS-SIS, in order to improve its utility and accuracy, and provide consolidated services.

In the last section we present the final conclusions of the report.

6. Current CS-SIS since 2013

At present, the SIS works under the first Regulation and Decision and the system put in production since 2013. According to that Regulation, 6 articles allow the end-user to create person-related alerts and consult the CS-SIS (see **Figure 7** below). For further details on these articles, we refer the reader to the legislation, or to the 2015 DG JRC study on the AFIS for SIS [77] where a summary of the regulation can be found.

Figure 7. Present functionalities of CS-SIS in production since 2013 (Source: EC 2018).



The CS-SIS database can store person alerts which contain:

- Alphanumeric data.
- 10-print cards (images).
- Photographs and facial images.

Even though photographs and facial images can be stored as part of person-related alerts, the only data that can be used to identify a subject in CS-SIS (i.e., perform a consultation) are:

- Alphanumeric data.
- 10-print cards.

The use of 10-print cards for consultation of SIS implied the integration into its functionality of a **Biometric Matching System (BMS)** which, at the moment, consists only of an **Automatic Fingerprint Identification System (AFIS)**. The AFIS started its roll-out phase in March 2018 with 8 MSs and one associated State connected to it. The BMS database contains only the extracted biometric templates from the 10-print cards.

The fingerprint images are stored together with alphanumeric data in the CS-SIS DB and once the biometric templates are created and are not "visible" to the BMS.
The link between the fingerprint images and the templates extracted is established via Unique ID (UID) associated with the alert. These templates are used by the AFIS search engine to consult the database. Therefore, as shown in **Figure 7**, the SIS contains two different databases with biometric data:

- **CS-SIS DB**. The first database stores the original biometric data sent by the MSs to the central SIS. This is the CS-SIS DB which contains the alerts related to persons. Regarding biometric data in particular, this database contains fingerprint images and face images (in addition to the alphanumeric data).
- **BMS DB**. The second database is associated to the BMS and stores automatically **searchable templates**. At the moment, only templates coming from TP cards are extracted and stored in this database for the purpose for biometric **10-print comparison**.

The CS-SIS is used in two main contexts which both present different operational requirements – law enforcement and the regular border crossing.

In the next subsections we describe the functioning of the current CS-SIS in each of these use-cases, with respect to the identification of subjects using biometric data, that is, their 10-print information (which is the only biometric information that can be used at the moment for identification purposes).
In the following sections of the report the terms "match" and "hit" are used according to the definitions given in Article 3 in the Police and Border new SIS Regulations from November 2018 (see section I for further details on this new regulation):

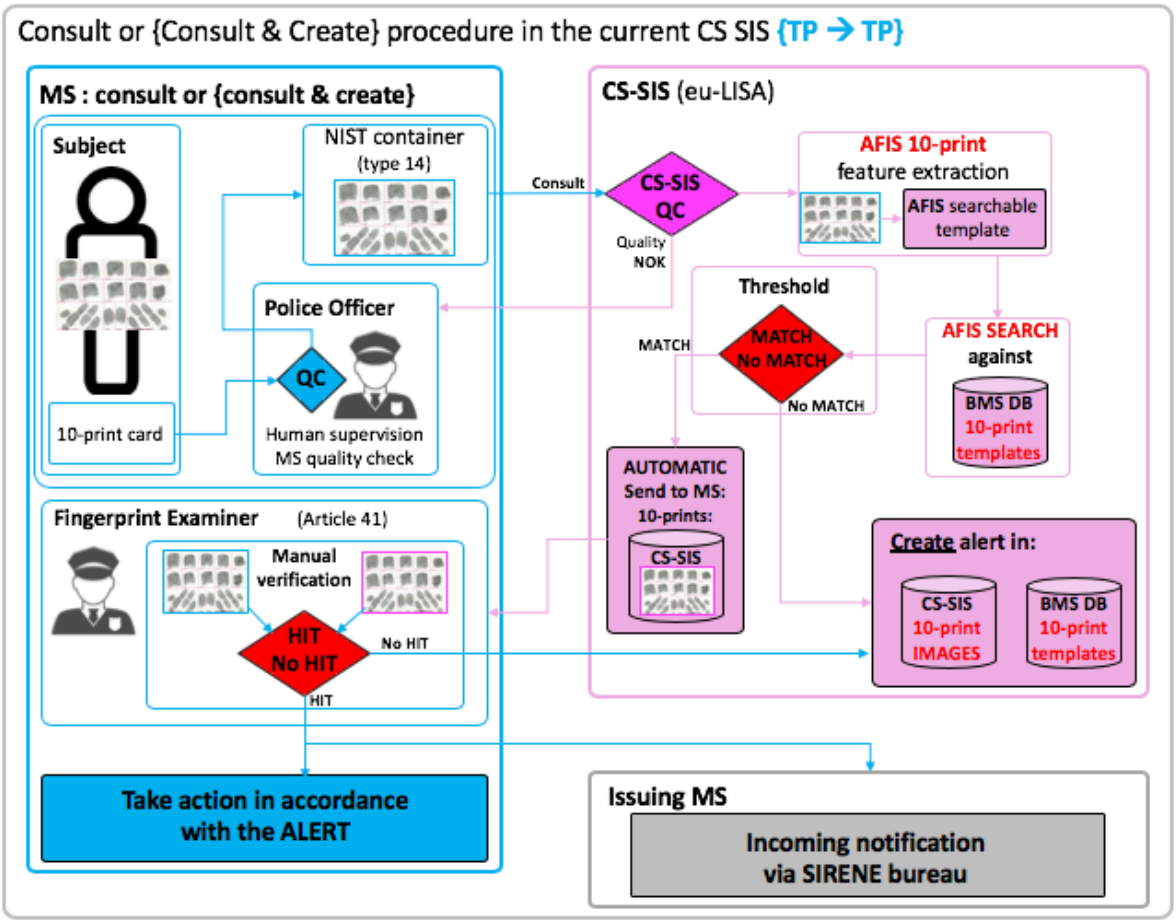
- **Article 3 Border, Police; Definition (7)**: a '**match**' means the occurrence of the following steps:
    - a search has been conducted in SIS by an end-user;
    - that search has revealed an alert entered into SIS by another MS;
    - data concerning the alert in SIS match the search data;

- **Article 3 Border, Police; Definition (8)**: a '**hit**' means any match which fulfils the following criteria:
    - it has been confirmed by:
        i. the end-user; or
        ii. the competent authority in accordance with national procedures, where the match concerned was based on the comparison of biometric data;
    - further actions are requested;

6.1. Current use of SIS in a law-enforcement context

According to the legislation, the creation of alerts in CS-SIS is strictly in competence of national law-enforcement agencies. Every MS connected to CS-SIS is allowed to create alerts in the system following a *Consult and create* procedure. This means that, before creating a new alert related to a subject, the system conducts a search in order to verify if there is already an existing alert associated to that same subject. A typical law-enforcement use-case is illustrated in **Figure 8**.

Figure 8. Police – CS-SIS Consultation and Alert Creation procedure (Source: EC 2018)



As mentioned above, at the moment the consultation process with regard to biometrics involves only 10-prints and can be described as follows:

- The subject of the alert is booked at the police station. His/her 10-print card is acquired using live-scan devices (usual case) or the traditional, but nowadays less-used ink-and-paper process. Alternatively, if the subject of the alert is not available at the police station (e.g., alert regarding a missing person) the 10-print card may be extracted from the national registry (if available).
- The quality of the fingerprint images is usually verified at the level of the MS. Fingerprints which are not of sufficient quality can be re-enrolled (if the subject is present at the police station).
- Once the 10-print card has been created at the MS, it is submitted to CS-SIS using a dedicated NIST container (type 14).
- At CS-SIS it is checked that the NIST container is compliant with the specifications of central system. A biometric quality check follows in order to ensure that the quality of the fingerprint images is sufficient for the AFIS to extract a searchable template. In case that any of these two checks fails (NIST container compliance or minimum quality to extract a template), CS-SIS notifies the MS.

- If the templates are extracted from the 10-print card, the AFIS searches the BMS-DB containing the 10-print templates of person-related alerts existing in the system.
- The AFIS technology based on 10-print has shown to be accurate enough in order to pre-define a threshold, based on which the system can produce a match (if there is a comparison score above the threshold between the searched fingerprints and any of the templates in the BMS DB) or a no-match (if the comparison score is below the threshold).
- **No-match** means that there is no AFIS-searchable biometric template present in the BMS-DB which can be linked to the suspect. Following this outcome, the MS conducting the consultation has the option to create a new entry in SIS, where the 10-print card is stored in the CS-SIS 10-print image DB and the searchable templates are stored in the BMS 10-print template DB.
- **Match means** that an AFIS-searchable template corresponding to that of the subject of consultation was found in the BMS-DB. At the MS level, a forensic expert verifies the match by comparing the existing 10-print card in SIS to the 10-print card of the subject of the consultation. If the verification results in a **no-hit** (i.e., error of the AFIS system), a new alert can optionally be created in CS-SIS in an analogous way to the no-match case (described above). In case of a hit (i.e., existence of an alert in SIS related to the subject of the consultation), the MS acts according to the nature of the alert and the MS owner is notified of the hit through the Sirene Bureau.

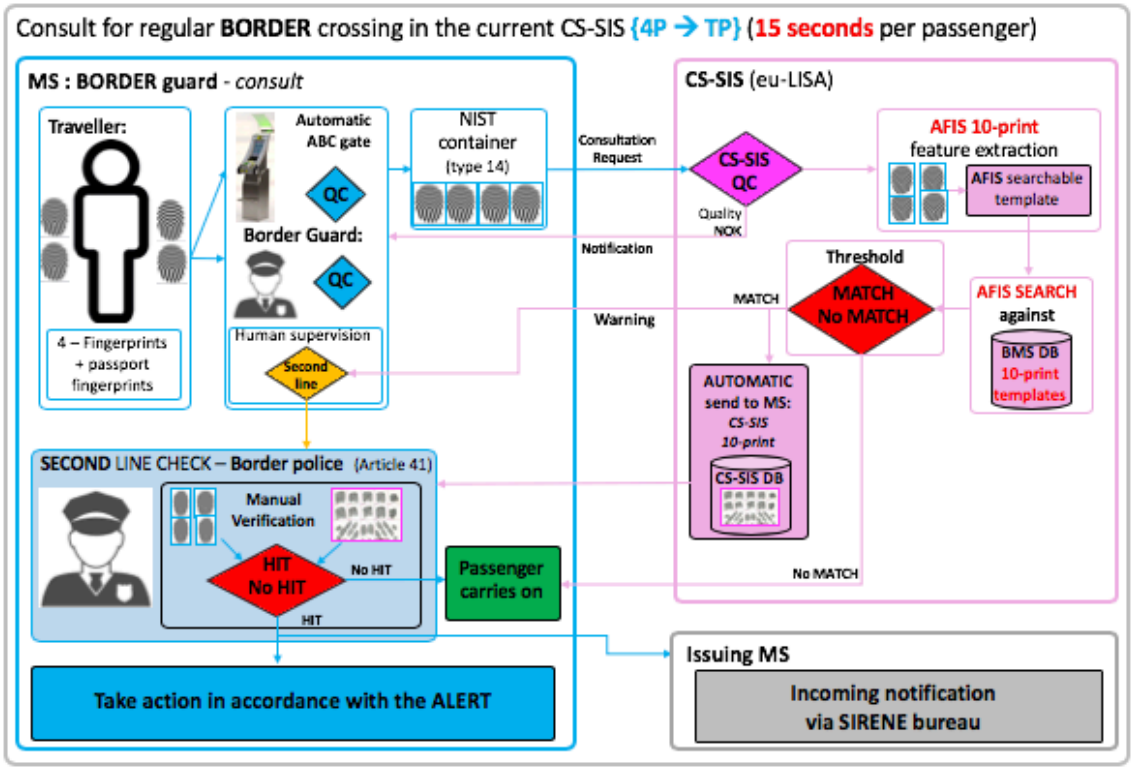
6.2. Current use of SIS in a border context

Although in principle this biometric use-case is allowed under both – first (2006 and introduction of an AFIS confirmed in 2016) and current (2018) Regulations – it is currently not exercised at the first line of check of regular border crossings due to the following reasons:

- Technical solution for automatic creation of CS-SIS compatible templates for border guards and for the ABC gates is yet to be implemented
- Technical solution for processing of automatic feedback provided by the CS-SIS (hit / no-hit) is yet to be implemented
- This use-case is yet to be tested and validated in operational conditions (pilot test-study is currently under development)

In the case of checks at regular border crossings, there are several differences to be taken into consideration with respect to the use of SIS in a law-enforcement use-case. The full "biometric" operation of SIS in this use-case is illustrated in **Figure 9**. In a border crossing, the subject of the consultation is a regular traveller, while in the context of law-enforcement the person is in general the suspect of some crime or illegal activity. In a border crossing, there is a strict limitation in terms of time for which the border guard can dedicate to each person.

Figure 9. Border – CS-SIS Consultation procedure (Source: EC 2018)



The border crossing should be as fast (and as efficient) as possible. In a typical law-enforcement use-case, the officers usually have a reason to stop the subject and time is usually not a first limitation to perform the necessary checks on the apprehended person.

In a regular border crossing use case taking place at the first line of check, it is foreseen that only consultations of the CS-SIS using the BMS-AFIS are performed and new alerts are not created in the system.

As mentioned above, at the moment, the consultation process with regard to biometrics involves a search against the 10-print card templates stored in the BMS-DB and can be described as follows:

- In this use-case, a subject who wants to enter the Schengen area arrives in front of a Border Guard or in front of an Automatic Border Checking (ABC) gate. Typically, the index and middle fingers of both hands are captured using a live-scan device, which can be used to consult CS-SIS after a sufficient image quality level has been reached. It should be noticed that the number of fingerprints acquired for the consultation can vary. It should also be noticed that although speed plays a significant role in this use-case (15s turnover to be guaranteed), quality of the fingerprints consulted from the border post against CS-SIS database should be verified and only "good quality fingerprints" should be submitted for consultation.
- The acquired fingerprints are embedded in a CS-SIS compatible NIST container (type 14) and transmitted to the CS-SIS for consultation, where two checks are performed: 1) the compatibility of NIST with the CS requirements; 2) quality of the fingerprints being of a level sufficient for feature extraction. In case either of these two checks is not successful, a notification is sent to the border guard.

- In case both of the previous checks are successful, a searchable template is extracted from the fingerprints and a search is conducted by the SIS AFIS on the BMS-DB (containing 10-print templates).
- The AFIS technology based on 10-print has shown to be accurate enough in order to pre-define a threshold, based on which the system can produce a match (if there is a comparison score above the threshold between the searched fingerprints and any of the templates in the BMS-DB) or a no-match (if the comparison score is below the threshold).
- No-match means that there is no AFIS-searchable biometric template present in the BMS-DB which can be linked to the suspect. Following this outcome, the border guard is informed and, if all other checks performed by the guard are also satisfactory, the person is allowed to enter the SCHENGEN space.
- Match means, that an AFIS-searchable template corresponding to that of the subject of consultation was found in the BMS-DB. The border guard sends the person to a second line of check where police officers can take more time to examine the case. A forensic expert verifies the match, comparing the existing 10-print card in SIS, to the fingerprints of the subject used to perform the consultation. If the verification results in a no-hit (i.e., error of the AFIS system), the person is eventually be allowed to carry on. In case of a hit (i.e., there is already an alert in SIS related to the subject of the consultation), the MS acts according to the alert and the MS owner is informed of the hit through the Sirene Bureau.

It is perhaps worthwhile to distinguish between the nature of the alerts in CS-SIS – in case of a *"discrete surveillance"* alert the passenger should be let free with no intervention at the second line, but the information that the person has passed the border crossing should be logged in the CS-SIS.

As stated in the current legislation, *"… Dactyloscopic data may be searched in all cases to identify a person. However, dactyloscopic data shall be searched to identify a person where the identity of the person cannot be ascertained by other means…"* (current legislation on Border, Article 33, paragraph 2). This implies that the search using biometric fingerprint data is preceded either by:

- absence of a travel document;
- detection of inconsistency in the biometric travel document;

or following:

- failed alphanumeric search;
- failed automatic fingerprint verification (1:1 comparison by ABC gate or border officer);
- failed automatic face verification (1:1 comparison by ABC gate) or visual inspection by border officer.

Recommendation 1:

Regular border crossing first line of check use-case 4P→TP use-case

In case ABC gates are used to process fingerprints of the travellers, we recommend implementation of liveliness detection to mitigate the possibility of a presentation attack.

If not the case yet, we recommend implementing automatic creation of CS-SIS compatible NIST containers for both border crossing scenarios (ABC gate and live-scan in front of the border guard), which is necessary for smooth interaction with the CS-SIS. If not the case yet, we recommend an automatic quality assessment to be implemented for both border crossing scenarios (ABC gate and live-scan in front of the border guard) to ensure, that only good quality fingerprints are consulted with the CS-SIS.

Given the strict time constraint at the first line of check, the border guard (or an ABC gate supervisor) should not be overwhelmed by an unnecessary amount of information. We recommend to make the feedback received from the CS-SIS as straightforward as possible, for example, no traveller-related information in CS-SIS (green light – traveller proceeds) and if information present in CS-SIS (amber light – traveller goes to the second line of check unless it is for discreet surveillance). We recommend that live-scan fingerprints are favoured over those stored in the passport.

7. New functionality of CS-SIS

Published on the 28th November 2018, the SIS revised legislation proposes 7 different alerts in which biometric data may be introduced to the CS-SIS (summarized below in **Table 6**).

Table 6. Articles containing alerts using biometric data in CS-SIS

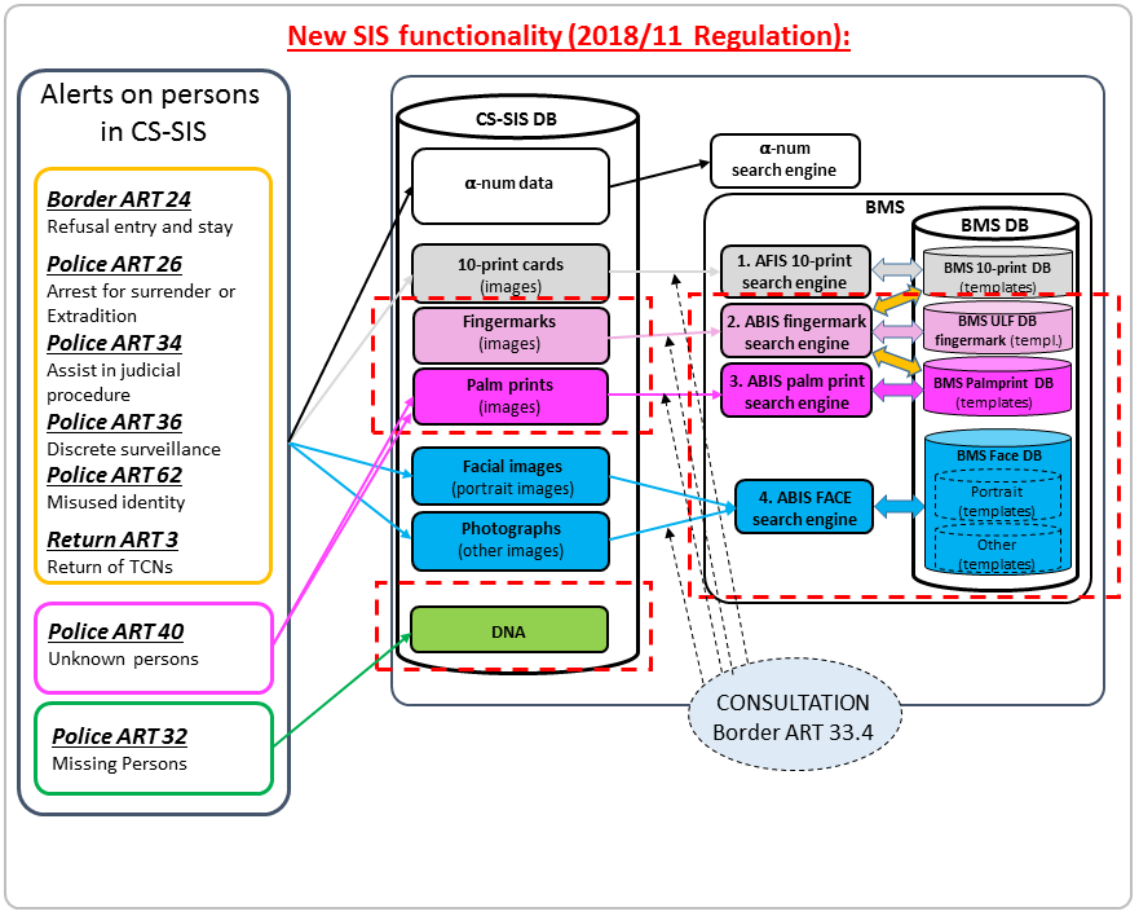
Article	Alert type
Border ARTICLE 24	Refusal of entry and stay.
Police ARTICLE 26	Alerts on persons wanted for arrest, surrender or extradition.
Police ARTICLE 34	Alerts on persons sought to assist with a judicial procedure.
Police ARTICLE 36	Alerts on persons and objects for discreet checks, inquiry checks or specific checks.
Police ARTICLE 62	Additional data for the purpose of dealing with misused identities.
Police ARTICLE 40	Alerts on unknown wanted persons for the purposes of identification under national law.
Police ARTICLE 32	Alerts on missing persons or vulnerable persons who need to be prevented from travelling.
Return ARTICLE 3	Alerts on the return of illegally staying third country nationals.

In light of the above-mentioned articles, the CS-SIS is to be enhanced by new functionalities (see **Figure 10** below). According to this legislation, the main new biometric functionalities with respect to the previous Regulation can be summarised as follows:

- A new type of alert related to "unknown persons" is introduced in article 40 (POLICE document). As a result, two new biometric characteristics are introduced: fingermark and palmmark (to allow searching for unknown persons).
- A search engine is to be added for automatic face recognition whenever the technology becomes ready (the storage of facial images and photographs was allowed under previous legislation already).
- In the case of missing persons, if fingerprints or facial image(s) are not available, the storage of DNA profiles is to be allowed (subject to an independent readiness and availability assessment).

The MSs' are now allowed to search the CS-SIS ABIS in parallel with the search on their national system (Recital 21 of the Police cooperation document). This slight, yet important change in the legislation may (will) in principle result in increased traffic in terms of CS-SIS consultations.

Figure 10. New functionalities of CS-SIS according to the 2018 Regulation (Source: EC 2018)



Similarly, as in the present architecture of the SIS, depicted in **Figure 7** (section 6), there are two blocks at the CS-SIS level, the CS-SIS DB and the Biometric Matching System (BMS) DB. However, based on the new 2018 legislation, these two blocks will be now substantially updated:

- The Central System Database (CS-SIS DB), stores alphanumeric data, facial images, photographs, 10-print cards, palmprints, fingermarks, palmmark and DNA profiles.
- The Biometric Matching System (BMS) DB is formed by:
- BMS databases which will contain searchable templates, extracted from the different biometric modalities: 10-print, Face (mugshots and other type of images), Fingermark (Unsolved Latent Files, ULF), Palmmark or Palmprint.
- Number of biometric search engines that will perform the consultations on the BMS DB: AFIS 10-print, ABIS-fingermark, ABIS-palmmark, ABIS-palmprint and ABIS face.

The link between the alerts stored in the CS-SIS DB and the BMS-DB is the Unique ID (UID) and for the purpose of comparison the BMS search engine only interacts with the templates stored in the BMS DB.

Some of the technology providers mentioned a multi-level search option integrated in their ABIS-fingermark search algorithms. These would however require access to the

fingerprint / fingermark images stored in the CS-SIS DB – a functionality which is not granted under current legislation. They presented a following reasoning:

- Fingermark comparison algorithm produces a ranked shortlist of candidates at the first level.
- At the second level the comparison algorithm retrieves the fingerprint images of the short-listed individuals for more detailed comparison, in which the "texture" components of the friction-ridge image are used for comparison.
- Given the advances in the Deep Learning and Artificial Intelligence, the **friction-ridge image** becomes a **"feature"** in the latest generation of ABIS algorithms. In order to fully utilise the capacities and capabilities of the latest-generation ABIS technology and to avoid the limitation of using template-only search, it is therefore desirable to allow the ABIS algorithms access to the CS-SIS image DB.

The result of this multi-level search is a boost of performance in terms of rank-1 accuracy (gain not quantified) and potential elimination of false positives, while still operating in the fully automatic mode.

Interaction between the search engines and the databases.

- ABIS 10-print search engine interacts with:
  - BMS 10-print templates DB
  - Can in principle interact with the BMS ULF fingermark and palmmark template database, under the assumption that the templates are compatible which is not the case yet (all of the 10-print fingerprint images from the CS-SIS have to be reprocessed in order to be compatible with ABIS Fingermark search engine to be selected).
- ABIS Fingermark search engine interacts with:
  - BMS Unsolved Latent Files (ULF) fingermark and palmmark templates database.
  - BMS 10-print template database.
  - BMS Palmprint template database (similar as in the previous case, all the palmprint images stored in CS-SIS have to be processed to be ABIS fingermark search to be selected).
- ABIS Palmprint search engine interacts with:
  - BMS palmprint template database
  - Interact with the BMS ULF fingermark and palmmark template database as long as the templates are compatible
- ABIS Face search engine interacts with:
  - BMS face image database of mugshots (high quality, high resolution, full frontal, controlled conditions acquired photographs)
  - BMS face image database of other faces of lower quality, produced in uncontrolled conditions, though still showing "sufficient resolution" to produce an ABIS-searchable template (e.g. webcam, CCTV, photograph, etc). Please see below for further details

NOTE: The 10-print templates, which are currently stored in the BMS database, are ***not fully compatible*** or ***optimised yet*** with fingermark / palmmark search and will **have to be reprocessed**. This procedure is ***inevitable***, whether it is decided to keep the

current system of the 10 prints AFIS or proceed with any other system to implement a solution for fingermark / palmmark comparison.

Recommendation 2:

Dedicated search engines

We recommend maintaining a dedicated dataset of Unsolved Latent Files, which would be logically separated into fingermarks and palmmarks (if source is known) and marked source unknown otherwise.

We recommend to implement a dedicated search engine for fingermark → ten-print comparisons; ten-print → unsolved latent files comparisons; fingermark → unsolved latent files comparisons; palmmark → palmprint and palmprint → unsolved latent files comparisons.

Recommendation 3:

ABIS access to the CS-SIS ridge shape images

In order to take advantage of deep learning technologies, we recommend for the ABIS system to have access to targeted fingerprint and palmprint images stored in the CS-SIS, once the search-process on templates is completed and a rank list of candidates is produced (Face, Palmprint, ULF (Fingermark and Palmmark). The images of the palmprints / fingerprints of the rank-list of candidates, retrieved from the CS-SIS, would be used in a subsequent cascade search in which the images themselves would become the source of new texture features and thereby make the search results more accurate.

Recommendation 4:

Need for complementary statistics

Upon implementation of ABIS-fingermark and Palmmark search engine, we recommend following statistics be likewise collected from the Central System and National copies of the SIS: the number of consultations performed based on the ABIS-fingermark and Palmmarks; the number of person related alerts that contain fingermark images (Art. 40); the number of hits produced by the ABIS-fingermark search engine; the number of duplicated alerts detected by the ABIS-fingermark search engine; the quality of the enrolled fingermark images in CS-SIS; the quality of the fingermark images submitted to perform consultations in CS-SIS.

Recommendation 5:

Benchmark test datasets built on SIS data

We recommend regular (every major update of the ABIS system used, but also periodically every 3-5 years) benchmark performance evaluations, after a first performance assessment of participating technology providers to be a part of the call-for-tender before selecting a new ABIS technology.

For this purpose, we recommend to develop and maintain, with the direct participation of the Member States (responsible of the data) a dedicated benchmark database with known ground truth for all kind of friction-ridge modalities based on the real data of SIS.

Recommendation 6:

Friction ridge image resolution

We recommend the fingermark and palmmark images to be stored in 1000dpi (or higher) resolution. As confirmed by the different vendors, the current COTS algorithms are capable of processing dactyloscopic traces in this resolution.

Note: In case when the reference database is recorded (and maintained) at 500dpi, the higher resolution fingermarks and palmmarks are simply down-sampled.

At the moment, the exchange of data in the SIS system is done on slightly modified version of the ANSI/NIST ITL 1-2011 containers type 10, as required by the SIRENE manual. This standard does however not account for "future developments" in the domain of ridge flow biometrics (new types of features, texture descriptors, comparison algorithms etc.).

Recommendation 7:

Common interchange standard

We recommend adhering to the ISO 39794 biometric standard for exchange of minutiae and EFS, which will be sustainable in the long term. This standard accounts for future developments in the areas of feature extraction and comparison and ensures forward-backwards template compatibility.

Recommendation 8:

Parameters for evaluating accuracy of ABIS system

We recommend to clearly define a set of parameters that will be used in the evaluation of the overall performance of the ABIS-system.

Note: The parameters should be set together with the supplier(s) of the ABIS-Fingermark system, ideally in the call-for-tender technology benchmark evaluation test, as they will form "implementation" requirements and guarantee a certain level of accuracy of the ABIS system. An example of such requirement is a False Positive Identification Rate, FPIR=0.001% in a DB of 100.000 reference images.

8. Integration of an ABIS Fingermark and Palmprint in CS-SIS

According to the Art. 40, Member States have the opportunity to create alerts on ***unknown persons*** using full or partial fingerprints and palmprints (fingermarks and palmmarks), which are recovered either at a scene of serious crime or a terrorist offence. These can however be "*entered into SIS only when it can be established to a very high degree of probability that they belong to the perpetrator of the offence*".

The above-mentioned condition may be very hard, if not impossible to prove in some cases. It is typically possible to demonstrate that the fingermark / palmmark are part of the crime scene, if the quality of the mark allows, it is likewise possible to establish the link between the mark and the suspected individual. However, proving the intentional deposition of the mark by the suspect, for example on a murder weapon, his involvement in the offence and activity (e.g. stabbing the victim) is more challenging. It will rely on the careful analysis of the forensic expert who will analyse the context and possible dynamic of the crime scene.

We split the possible use-cases into two main subgroups – distinguishing between the law enforcement and regular border crossing applications. Nomenclature used in the use cases in this section is closely following the nomenclature used in the legislation adopted in November 2018.

8.1. Fingermark use cases

Several use cases can be defined for the interaction between the ABIS fingermark search engine and BMS databases in the context of ***Law Enforcement***:

- Fingermark template against BMS 10-print template DB (LP → TP)
- Fingermark template against BMS Palmprint template DB (LP → PP)
- 10-print template against BMS-ULF fingermark / palmmark template DB (TP → LP)
- Palmprint template against the BMS-ULF fingermark / palmmark template DB (PP → LP)
- Fingermark template against BMS-ULF fingermark / palmmark template DB (LP → LP)

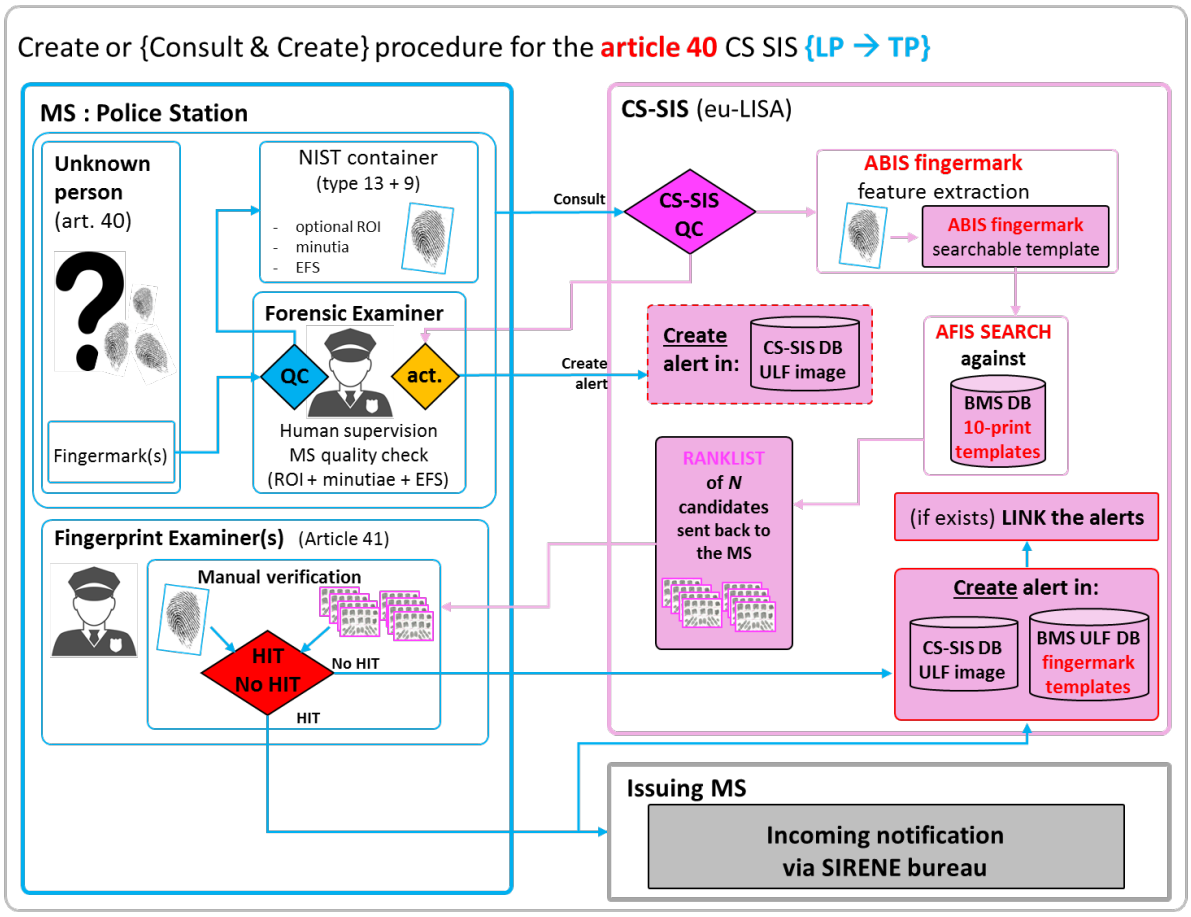
In the context of first line of check of regular ***Border*** crossing following use case can be envisaged:

- 4-print template against the BMS-ULF fingermark / palmmark template DB (4P → LP)

8.1.1. Law enforcement use-cases LP → TP

This use-case describes a fingermark versus a ten-print database search. For the purpose of this use-case we assume that the fingermarks at the police station already exist in their digital form.
Fingermark(s) from the crime scene are processed by the national forensic laboratory at the level of MS, analysed and searched on the national ABIS-Fingermark system. In parallel, the MSs' are given the opportunity to launch a search on the CS-SIS in a process depicted in the **Figure 11** below.

Figure 11. Fingermark vs. BMS 10-print Template Database (Source: EC 2018)



The quality level of the partial friction ridges (sometimes is not possible to distinguish, which friction ridge created the trace - finger, palm, sole, toe) is verified in the analysis phase and if it has Value for Comparison (VC) it can be submitted to CS-SIS for consultation (or consultation and creation). This way the "***garbage in, garbage out***" effect is mitigated.
The consulting officer at the level of the MS should be aware, that any consultation with fingermarks will produce a rank-list of candidates, which will have to be verified at the level of the consulting MS. The system will not return a binary response in a form of "hit – no hit" like in the case of ten-print to ten-print comparison.

The consulting officer has several possibilities:

- Place into the CS-SIS specific NIST container only a fingermark image (type 13) with marked ROI. The ROI mark-up process should be documented by the ABIS-Fingermark system provider. The automatic feature extraction, EFS extraction and template creation occurs at the side of CS-SIS.
- Accompany the fingermark image (including ROI – type 13) with minutiae and Extended Feature Set (EFS) – type 9, which are manually marked using the NATIONAL ABIS system.
- Accompany the fingermark image (including ROI – type 13) with minutia and EFS – type 9, which are automatically extracted by the NATIONAL ABIS system and fingerprint examiner operator verified.
- Accompany the fingermark image (including ROI – type 13) with minutia and EFS – type 9, which have been automatically extracted in a „fully lights-out" mode using the National fingermark ABIS.

The CS-SIS NIST container is submitted to the CS-SIS. At the receiving point, next to the integrity check on the entire NIST container, the fingermark image quality is assessed, in order to ensure that sufficient level of features is present in the fingermark in order to produce a BMS-searchable template.

If the fingermark is not of a sufficient quality, the CS-SIS should reject the fingermark and send an automatic notification to the consulting MS.

If the BMS fingermark template is extracted, it is searched against the BMS 10-print template database (LP → TP search). This search produces a rank list of candidates.

Since NO images / 10-print cards are stored in BMS (it contains only templates)itself, actual 10-print cards of the candidates listed need to be extracted from the CS-SIS Data Base using the UID's as a reference and transferred to the MS for verification. At the national level the fingermark is compared against the returned *N-candidate list* and the fingerprint examiner(s) should reach a **HIT** / **NO-HIT** (or **INCONCLUSIVE**) decision.

In case of **NO-HIT**, the consulting officer may create an alert on the fingermark, which will be stored in the CS-SIS (fingermark image) and BMS-ULF fingermark and palmmark template database. In case of a **HIT**, the MS owning the alert on 10-print card is notified via SIRENE bureau, with option to link the two alerts (in case an alert is created).
Alternatively, in case of a NO-HIT, the fingermark should be searched against the palmprint database as well as it may have originated from a palm.

Recommendation 9:

Fingermark image quality metrics

We recommend, when technology becomes available, the implementation of fingermark quality assessment (Fingermark Quality Metric) into the CS-SIS processing pipeline.

In cases strictly linked to the Art. 40 we recommend to allow the MSs to create alerts using fingermarks of "insufficient" image quality (e.g. ABIS not capable of producing a biometric-searchable template), as these may become "searchable" in the (near) future.

Some of the technology providers have suggested to adopt a different approach to evaluate the quality of the fingermarks / palmmarks at the level of MS. That is, to set a minimum number of minutiae. Global consensus amongst the technology providers is that at least 3 minutiae should be present in order for the ABIS-fingermark to produce a searchable template.
Note: Although 3 minutiae may be sufficient to **consult** a fingermark (e.g. to perform automatic feature extraction and create an ABIS-searchable template), it may ***NOT HAVE SUFFICIENT*** discrimination power necessary to identify an individual in the context of national law. It is therefore advisable to **create alerts** with fingermarks, in which six or more minutiae are present (given the technology available at the date of publication of this report).

Recommendation 10:

ROI and number for fingermarks per SIS consultation

It has been suggested by some providers and users, that fingermark and palmmark feature extraction and comparison algorithms may perform more efficiently if one single fingermark is present in the image submitted. We recommend cropping the image containing fingermark to the ROI, in cases when multiple fingermarks are present in the image.

Recommendation 11:

Quality check in absence of Quality Metric

In the absence of robust and reliable fingermark / palmmark image quality metric we recommend to:

- Identify and share best practices applicable to SIS between MS and maintain a common repository of these best practices.
- Use the National AFIS in an attempt to produce a NS-AFIS searchable template. Should a National AFIS be capable of producing a template, the ABIS-fingermark and palmmark implemented at the CS-SIS should "in principle" be capable as well of producing an ABIS-searchable template.
- Allow the MS to finalise the creation of an alert (art. 40) with a fingermark/palmmark which failed to produce an ABIS-searchable template. The alert will be flagged as not searchable but it is likely that forthcoming technology development will allow extraction of ABIS-searchable template from these images in the near future.

Recommendation 12:

Rank list size and feedback from the CS-SIS

Given that the operating parameters of the fingermark and palmmark ABIS are yet to be defined (or they will become known after a benchmark vendors evaluation is performed during the call-for-tender), we recommend to fix by default the number of returned candidates to 20 (which constitutes a conservative average observed during the visits at national laboratories). A possibility should be given to the consulting officer to request a longer rank list. We further recommend that the rank lists are completed with comparison scores.

Note: Once the performance parameters of the implemented technology are known, the rank lists could be converted into "dynamic". The size of such a rank list could be calculated for example as a function of distance of rank 1 score to the cohort of nearest 5 ranks.

Recommendation 13:

Use-case LP → TP

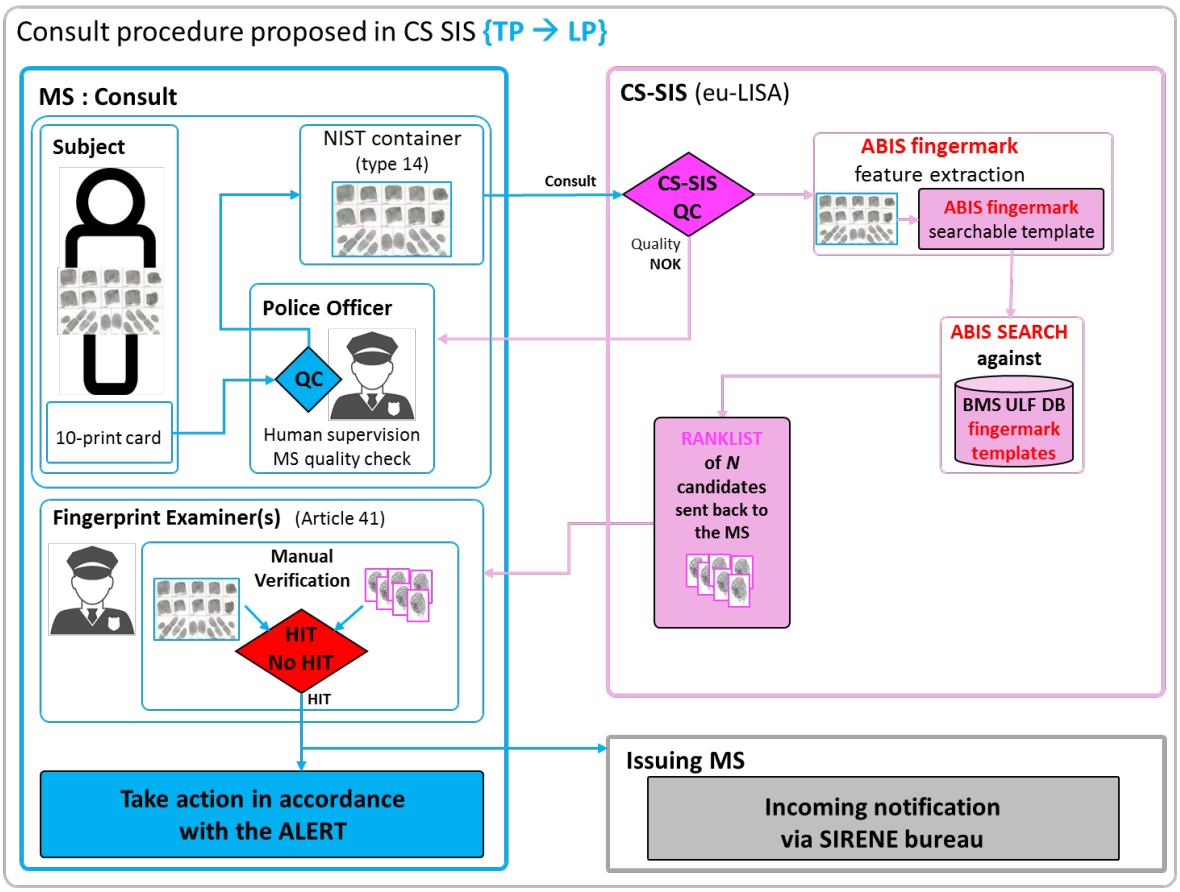
In case of a **No-Hit,** the consulting officer should re-label a fingermark as a palmmark, as the "alleged" fingermark may have originated from a palm and thus may produce a hit in the BMS-palmprint database. Alternatively, it could be possible to search immediately on both.

We recommend using a dedicated ABIS feature extraction algorithm, which is capable of extracting the fingermark-searchable templates from fingerprint images for creation of the alerts in the BMS-ULF.

8.1.2. Law enforcement use-cases TP → LP

This use-case describes a 10-print versus an Unsolved Latent Files (ULF) database search. Once a person is booked at the police station, his fingerprints can be searched against a database of Unsolved Latent Files (see **Figure 12** below). As mentioned earlier, if allowed by the MSs' national law, the search in CS-SIS can occur in parallel with the search on the national ABIS ULF and TP database.

Figure 12. 10-print vs. BMS database of Unsolved Latent Files (Source: EC 2018)



TP's of the person are collected (rolled or flat / inked or live-scan) and following a quality check at the level of MS are submitted to CS-SIS in a NIST container. At this stage, having the person in custody, it is possible to re-acquire / re-enrol the TP's in case the quality is not satisfactory.

The first step at the CS-SIS is the "integrity" verification of NIST container, which should be accompanied by internal fingerprint quality check. At the level of BMS, ***fingermark searchable templates*** need to be extracted and the TP templates are searched against the BMS ULF fingermark template database. This search produces a rank-list of candidates and the remaining procedure is similar to the procedure highlighted in previous point (9.1.1).

The search on BMS-ULF template database results in a rank-list of candidates which are linked with the corresponding fingermarks stored in the CS-SIS fingermark database via UID. These are returned to the consulting MS who is responsible verification, which can conclude a **HIT** / **NO-HIT** or **INCONCLUSIVE**.

In case of **NO-HIT** the MS proceeds according to their business as usual (BAU) procedure.
If a hit is confirmed, there is in principle no need to create an alert or establish a link to a previous alert. Since the person is in the custody and his identity is known, the consulting MS acts in accordance with the alert and notifies the owner of the alert via SIRENE bureau.

Recommendation 14:

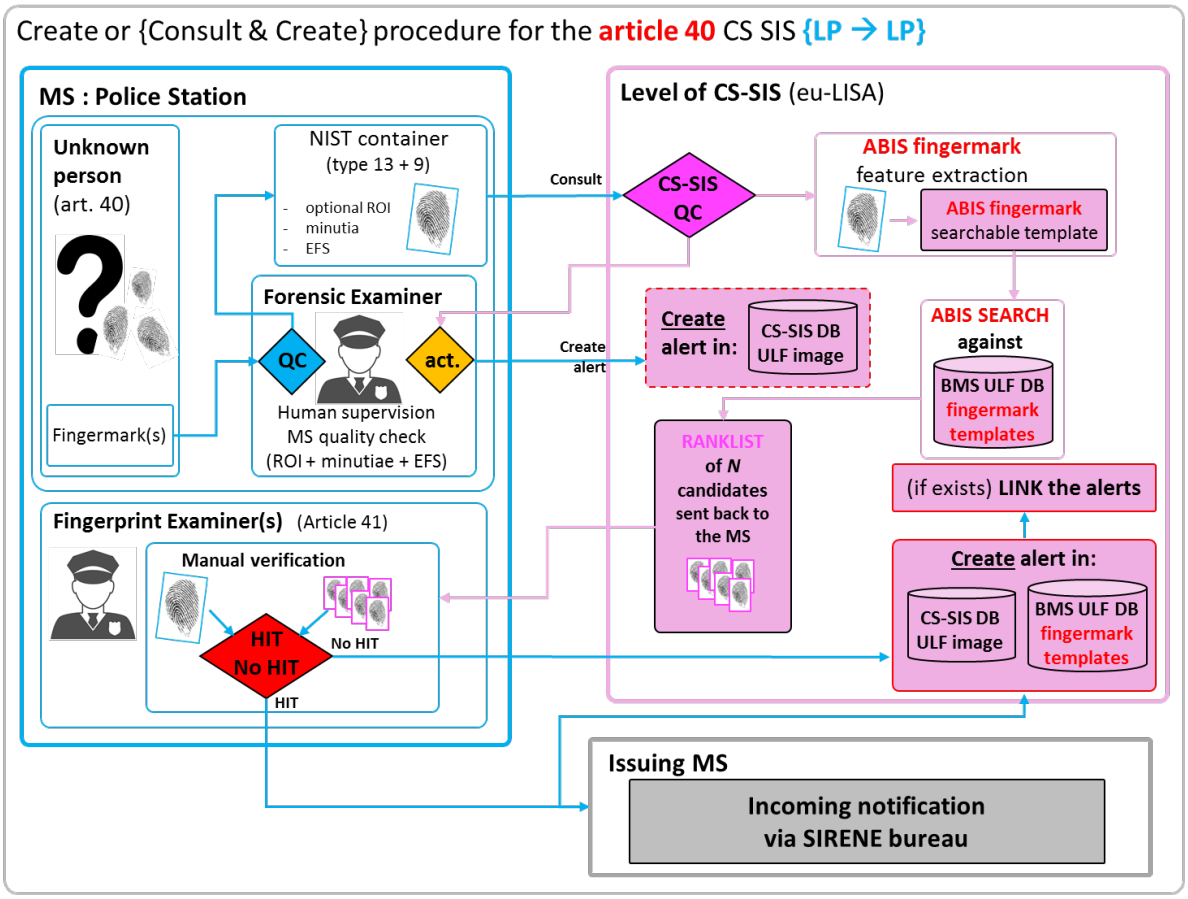
Use-case TP → LP

We recommend using a dedicated ABIS search algorithm that is capable of extracting the fingermark -searchable templates from ten-print fingerprints to consult BMS-ULF database.

8.1.3. Law enforcement use-case LP → LP

The initial part is identical to the previous use-cases and varies at the point of ABIS fingermark / palmmark search (see **Figure 13** below). Although only fingermark search is shown, the process of LP → LP search with palmmark is identical. Unlike in the previous use-cases (section 8.1.1 and 8.1.2), the fingermarks and palmmarks in this use-case are searched against the BMS-ULF fingermark and palmprint template database.

Figure 13. Fingermark vs. BMS database of Unsolved Latent Files (Source: EC 2018)



It should be noted here, that although the LP → LP searches are technically feasible, they are not routinely performed at the level of MS, due to time constraints or additional manpower necessary to verify every returned rank-list of candidates. Worth mentioning is the fact, that in this particular use-case the identity of the person is unknown, as is the identity of the persons in the BMS-ULF fingermark and palmmark database, the aim with this use case will therefore not be an identification but the creation of links between different cases involving potentially the same suspect.

The search on BMS-ULF template database produces a ***rank-list of candidates***, which are linked with the corresponding fingermarks stored in the CS-SIS fingermark database via UID. These elements are returned to the consulting MS who is responsible verification, which can result in **HIT** / **NO-HIT**.

In case of **NO-HIT** the consulting officer may decide create an alert, which will produce an entry in the CS-SIS fingermark image dataset and entry in the BMS-ULF template database if the article 40 criteria are met.
In a rather unlikely (but still possible) event of a **HIT** on a BMS-ULF database, the owner of the previous alert is notified via SIRENE bureau. The consulting officer in this case can update previous alert or introduce a new one and establish a link with the previous alert, assuming that they will be of equal importance (art. 40). The latter implies creation of an entry in the CS-SIS fingermark image database and a template in the BMS-ULF fingermark and palmmark template database.

Although this type of search might not reveal an identity of an individual (by definition the ULF alerts are of unknown wanted persons), the fingermark to fingermark HITS establish links between the alerts and thus provide potentially interesting investigation leads.

If allowed, the batch-consultations by MSs should occur in "off-peak" periods (when the ABIS systems are not used to full capacity) according to a rota-schedule to avoid creation of bottle necks (could occur if all the MSs decide to batch-consult the ABIS systems at the same time). This process could be automated at the level of MS.

Recommendation 15:

Use-case LP → LP

We recommend that the real-time Fingermark to ULF database search should be reserved for extreme cases of high threat of terrorism and/or serious criminal activity.

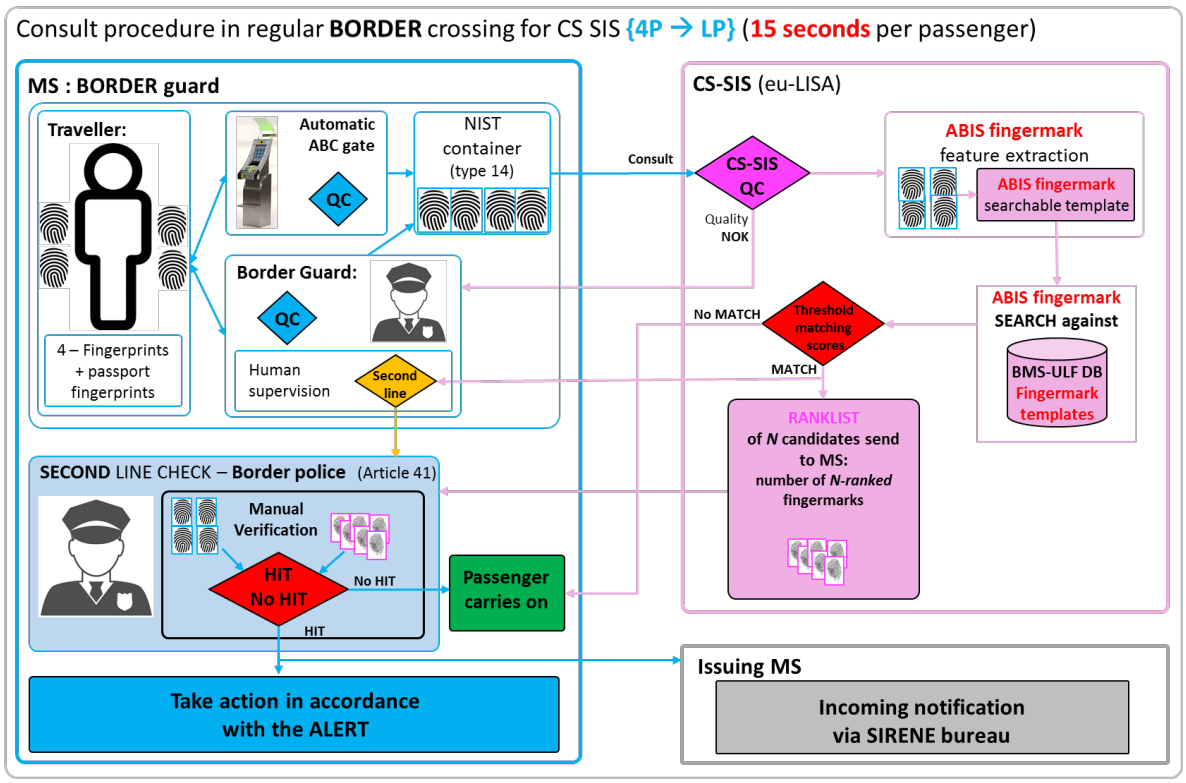
We recommend performing a batch comparison of unsolved fingermarks with the ULF database periodically, sort the candidates by the highest score and apply a pass threshold to reveal potential matches in the BMS-ULF database.

8.1.4. Regular border crossing use-case 4P → LP

In the context of regular border crossing depicted in **Figure 14** below, the key limiting factor is the time per traveller turnaround, together with the fact that a border guard at first line of check might usually not possess necessary skills for a full dactyloscopic examination. As already highlighted in section 6.2, if a biometric key to the passport is available, there is a choice between (up to) 4 fingers live-scanned fingerprints and the fingerprints stored in the biometric passport. Whenever available, the live-scanned fingerprints should be used. This use-case is computationally less intensive as the TP → TP use-case mentioned above. Nevertheless, there is a potential risk of False Rejections in case of mislabelling of fingers in the CS-SIS database.

Note: The 4P → LP use-case may result in no-match more often than TP → LP search, due to the fact that only 4 fingers are captured.

Figure 14. Border control (up to) 4 fingerprints vs. BMS database of Unsolved Latent Files (Source: EC 2018)



Whether in front of the border guard, or in front of the ABC gate, the quality of the scanned fingerprints should be verified and if satisfactory (rec. 12), they should be placed in an **automatically** created NIST container accompanied by alphanumeric data (rec. 15).

Internal quality check is performed at the level of CS-SIS and if fingerprints are not received, their quality is insufficient or there is something wrong with the incoming NIST container, the border guard (or the border guard supervising the ABC gate) will be notified. After being checked against alert containing 10 prints (see section 6.2) the 4P fingerprints are searched against the BMS_ULF fingermark and palmmark database. In order to ensure "smooth" processing of travellers like for the 4P→TP scenario, the only feedback the border guard (or the ABC gate) at the **first line** of check should receive from the CS-SIS is:

- No traveller-related information in CS-SIS (**green light** – passenger proceeds)
- Information present in CS-SIS (**amber light** – passenger goes to the **second line** of check)

In order to ensure the functionality in this scenario a ***high decision threshold*** shall be put in place for this transaction. Searches on BMS-ULF database ***always*** produce a rank list of candidates, which the border guard at the first line of check ***does not have time (or skills) to evaluate and process***. If a high decision threshold for the border application is not adopted, every single traveller, whose 4P's will be searched against the ULF, will be sent to the *second line* of check.

The search on BMS-ULF template database in this case would produce a "***PSEUDO MATCH***", still accompanied by a rank-list of candidates (it is likely that more than one candidate is matched above the threshold defined), which are linked with the corresponding fingermarks stored in the CS-SIS fingermark database via UID. These are returned to the consulting MS border for second line verification, which can result in **HIT** / **NO-HIT** or **INCONCLUSIVE**. In case of **NO-HIT** the traveller carries on.

Since the traveller is in custody at the second line and his identity is known, the consulting MS border police officer acts in accordance with the alert and notifies the owner of the alert via SIRENE bureau.
In the absence of a fingerprint examiner at the border, which is the case in vast majority of the border crossings, we recommend that use-case is reserved and practiced in the cases in which the EU is at high alert of terrorism.
Another possibility for meaningful implementation of this particular use-case is for it to be exercised as a background check, in which the four fingerprints of all incoming travellers are searched against the BMS-ULF database, providing that a high decision threshold is applied. The risk of this third approach is that if the ABIS produces a hit, it may be too late to apprehend the owner of the consulted fingerprint. Nevertheless, priceless intelligence could be provided in terms of additional data – alias (alphanumeric data), face image, CCTV footage and others.

Recommendation 16:

Live-scan images in the 4P → LP use-case

Whenever possible, we recommend using live-scanned fingerprints instead of the fingerprints stored in the passport for CS-SIS consultation.

Recommendation 17:

Regular border crossing and high decision threshold for 4P → LP

From the operational point of view and given the two different applications – the law enforcement and the regular border crossing, we recommend using a "binary flag" to distinguish between the consultation originating at the border and at the police station. In case of border crossing, a high decision threshold should be applied when searching against the ULF, and the border guard should be informed of a pseudo-match only when an Art 40 alert is above this high decision threshold.

8.2. Palmmarks use-cases in CS-SIS

Several use cases can be defined for the interaction between the ABIS palmmark search engine and BMS databases in the context of ***Law enforcement***:

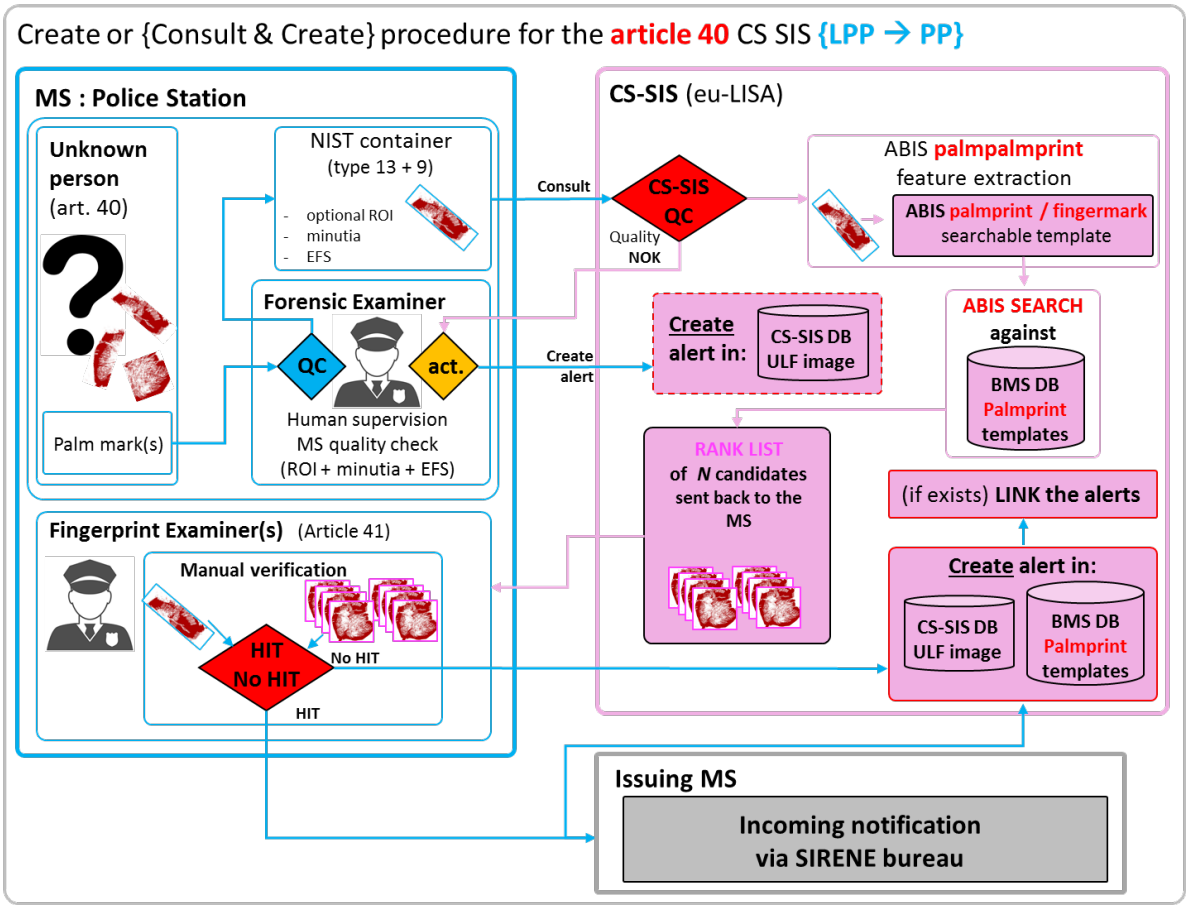
- Palmmark template against BMS Palmprint template database (LPP → PP)
- Palmprint template against the BMS-ULF template database (PP → LPP)

It should be noted here that the palmprints are not typically searched in the scope of the police investigation. They are mostly used when the fingerprints are unavailable, for example due to sickness or (non)deliberate alteration of fingerprints. In vast majority of cases the fingerprints (if available) are given the priority.

8.2.1. Police use-cases LPP → PP

LPP acronym derived from the term Latent Palm Print (covers Palmmarks recovered in the scope of police criminal investigation as well as partial palmprints).
Palmmark(s) from the crime scene are processed by the national forensic unit at the level of MS, analysed and searched on the MS national ABIS-Palmmark system and can be in parallel searched in the CS-SIS in a process depicted in **Figure 15** below.

Figure 15. Partial Palmprint / Palmmark vs BMS DB consisting of Full Palmprint templates comparison (Source : EC 2018, https://openclipart.org/detail/178364/red-palm-print)



Their quality should be checked prior to CS-SIS consultation (***Rec. 8***) keeping in mind the already mentioned „***garbage in, garbage out principle***". The consulting officer should be aware that any consultation with palmmarks will result in a rank-list of candidates, which will have to be verified at the national level.

The consulting officer has several possibilities:

- Place into the CS-SIS specific NIST container only a Palmmark image (type 13) with marked ROI
- Accompany the palmmark image (including ROI – type 13) with minutiae and Extended Feature Set (EFS) – type 9, which are manually marked using the NATIONAL ABIS system
- Accompany the palmmark image (including ROI – type 13) with minutia and EFS – type 9, which are automatically extracted by the NATIONAL ABIS system and human operator verified
- Accompany the palmmark image (including ROI – type 13) with minutia and EFS – type 9, which have been automatically extracted in a „fully lights-out" mode on the National fingermark ABIS

Possibilities 2-4 assume that the minutiae and extended feature sets are encoded in an interoperable way and are compatible with the SIS-BMS search (see section 9 on the interoperability).

The CS-SIS NIST container (type 13 and optional type 9) is submitted to the CS-SIS. At the receiving point, next to the integrity check on the entire NIST container, the palmmark image quality is assessed, in order to ensure, sufficient level of features is present in the palmmark to produce a BMS-searchable template.

If the palmmark is not of a sufficient quality, the CS-SIS should reject the fingermark and send an automatic notification to the MS.

Since the context of the art.40 alert is "serious crime" or "terrorist activity" and the palmmarks of "superior" quality cannot be acquired, MS consulting has the option to create an alert in the CS-SIS database. If the BMS palmmark template is extracted, it is searched against the BMS palmprint template database (equivalent to LP → TP search). This search produces a rank list of candidates.

Since NO images of the palmprint records are stored in BMS (it contains only templates), actual Palmprint images from the candidates listed need to be extracted from the CS-SIS DB using the UID's as a reference and transferred to the MS for inspection. At the national level the palmmark is compared against the ***N-candidate*** list and the forensic examiner(s) arrive to a **HIT** / **NO-HIT** (or **INCONCLUSIVE**) decision.

In case of **NO-HIT**, the consulting officer may create a new alert with the palmmark, which will be stored in the CS-SIS (palmmark image) and BMS-ULF palmmark template database. In case of a **HIT**, the MS owning the alert on Palmprint record is notified via SIRENE bureau.

Recommendation 18:

Dual use fingermark and palmmark in LPP → PP use-case

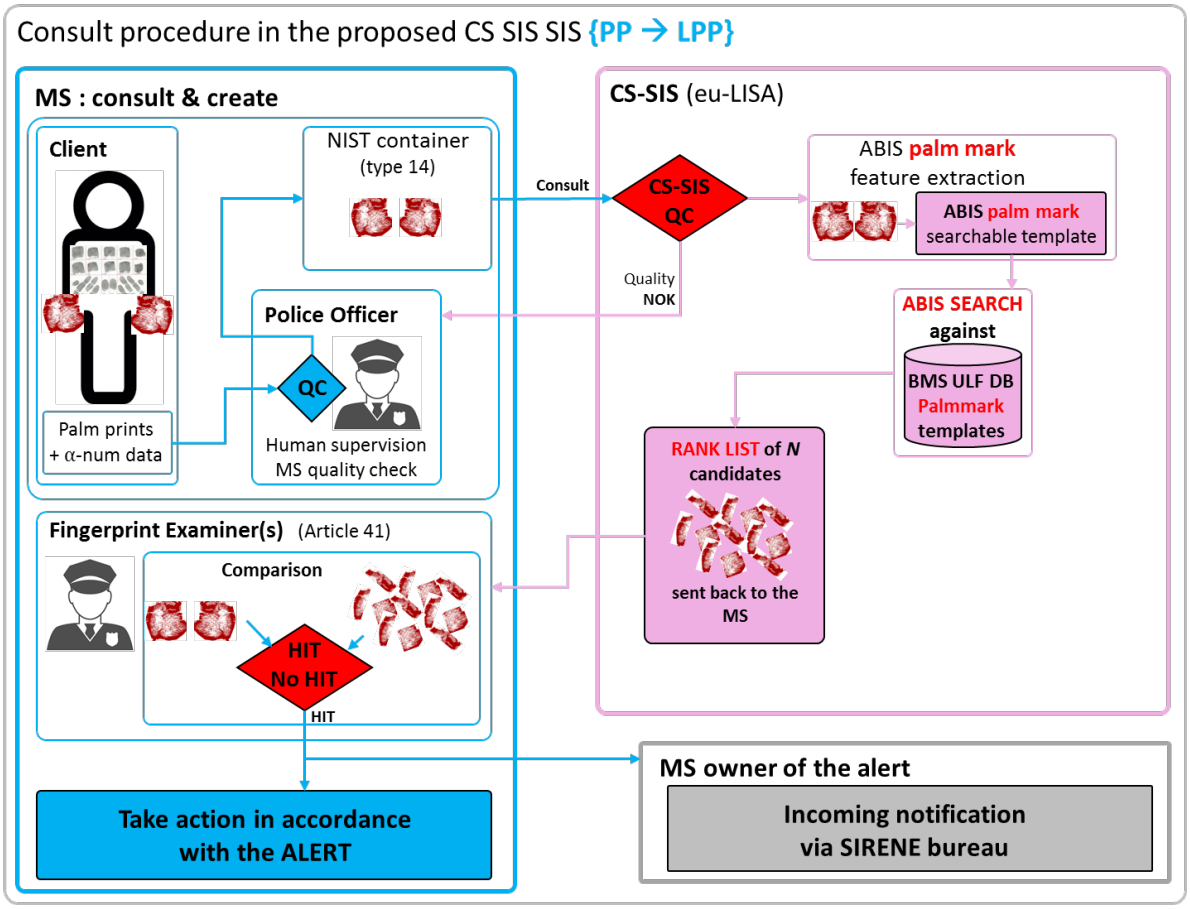
We recommend encouraging the consulting officer to encode an initially declared fingermark as a palmmark in case of a **No-Hit**, as the supposed fingermark might have originated from a palm and thus may produce a hit in the BMS-palmprint database.

We recommend using a dedicated ABIS feature extraction algorithm that is capable of extracting the palmmark-searchable templates from palmprint images for creation of the alerts in the BMS-ULF. (***recs. 9, 10, 11*** and ***12*** apply).

8.2.2. Police use-cases PP → LPP

Once a known person is booked at the police station, his/her palmprints can be searched against the ULF database (see **Figure 16** below) of the SIS.

Figure 16. Full Palmprints vs BMS database of Full Palmprints comparison (Source: EC 2018, Palmprint, https://openclipart.org/detail/178364/red-palm-print)



Palmprints of the person are enrolled (rolled or flat / inked or live-scan) and following a quality check at the level of MS are submitted to CS-SIS in a dedicated NIST container

(type 15). At this stage, having the person in custody, it is possible to reacquire the palmprints.

First step at the CS-SIS is an "integrity" verification of NIST container, which should be accompanied by internal fingerprint quality check.

At the level of BMS, ***palmmark search-compatible*** templates are used and the Palmprint templates are searched against the BMS ULF palmmark and fingermark templates database. The search on BMS-ULF template database results in a ***rank-list of candidates***, which are linked with the corresponding palmmarks stored in the CS-SIS palmmark database via UID. These are returned to the consulting MS who is responsible for the verification, which can result in **HIT** / **NO-HIT** or **INCONCLUSIVE**.

In case of **NO-HIT** the MS proceeds according to their business as usual (BAU) procedure and may decide to store the palmprints together with a newly created alert in the CS-SIS database.
If a **HIT** is confirmed, there is in principle no need to create an alert or establish a link to a previous alert, as the person is in the custody and his identity is known. The consulting MS acts in accordance with the alert and notifies the owner of the alert via SIRENE bureau.

Recommendation 19:

Use case PP→ LPP

We recommend using a dedicated ABIS search algorithm that is capable of extracting the palmmark-searchable templates from palmprint images for consulting the BMS-ULF database.

9. Interoperability

In the Initial Appraisal of the EC Impact Assessment on the Interoperability between EU information systems for security, border and migration management[45], released in February 2018, three different dimensions of interoperability have been identified – Technical, Legal and Political. This chapter focuses on the technical dimension of interoperability of CS-SIS from the perspective of dactyloscopic data (10-print fingerprints, up to 4 live scan fingerprints, fingermarks, palmprints and palmmarks).

From the point of view of the authors there are two, slightly different aspects of the interoperability: Interoperability at the MS national level and interoperability at the level of European Large-Scale IT systems. Both of these aspects will be addressed in the following sections.

Fingermarks, fingerprints and palmprints are processed at the level of MS on a national ABIS system, which will produce entries (such as biometric templates, minutiae, EFS) not necessarily compatible with the ones produced and stored in the Biometric Matching System (BMS) of CS-SIS. This can happen in a situation, when the national ABIS system was provided by a different vendor or even when the MS uses a different version of national ABIS system than the CS-SIS although issued by the same provider. This could lead to incompatibility of the features extracted from the biometric data.

9.1. Interoperability challenge between fingermark processed by MS and CS-SIS systems

Fingerprints, either originating from the 10-print cards, captured in the scope of police investigation or introduced by the live-scan devices, are in principle subject to fully-lights-out processing and as such, do not require additional human intervention. As underlined in the introduction of the report, this process is followed since March 2018 by the first 9 Schengen countries using the BMS of CS-SIS.

Fingermarks on the other hand usually require expert intervention related (but not limited) to manual minutiae mark-up, expert intervention on the automatically extracted minutiae points, extended feature mark-up, mark-up of ROI, etc.

From the moment the fingermarks are digitized and their quality verified by the dactyloscopic examiner, in principle only fingermarks of "Value for Identification" shall be introduced for search in the ABIS. However, several modes of interaction between the dactyloscopic examiner and the ABIS are possible, derived from the operational experiences observed at the level of MSs:

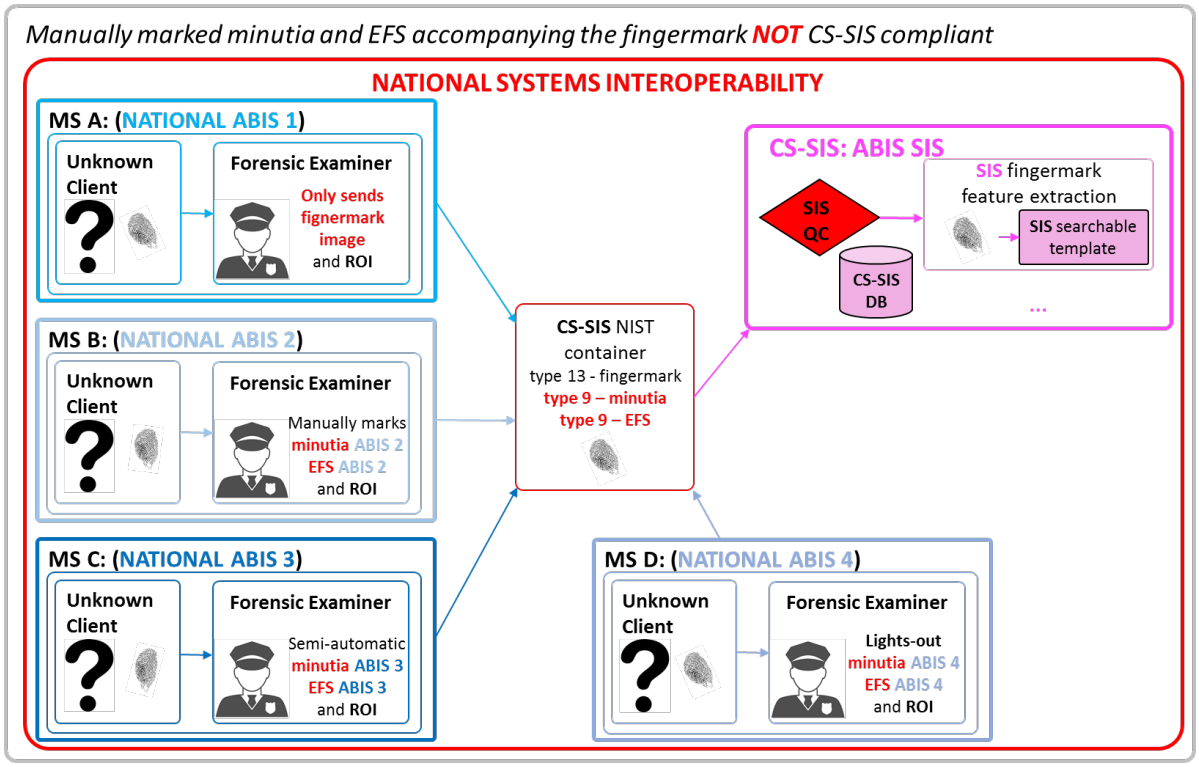
- **Case A**: Submit only fingermark with ROI (option strictly reserved to "high quality" fingermarks with second level features well defined)
- **Case B**: Submit fingermark with ROI and manually marked minutiae and / or extended feature set (EFS)
- **Case C**: Submit fingermark with ROI and automatically extracted minutia and / or EFS, which have been subjected to human verification

[45] http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/615649/EPRS_BRI(2018)615649_EN.pdf

- **Case D**: Submit fingermark with ROI and "lights-out" extracted minutia and / or EFS (no human verification)

Similar possible interactions can be envisaged with the CS-SIS fingermark ABIS (see **Figure 17** below), as long as the fingermarks (image with marked ROI), minutia points and EFS are placed in the CS-SIS compatible NIST container (type 13 for fingermark image and type 9 for minutia and EFS). These are transferred to the CS-SIS.

Figure 17. National Systems interoperability (Source: EC 2018)



It is more than safe to assume, that the minutia and features extracted by the CS-SIS ABIS will ***not*** be ***interoperable*** with the minutiae and features extracted by the MSs national ABIS. There are several different possibilities for addressing this:

Option A: **Use a fully lights-out mode.** This scenario keeps the potential burden incompatibility at the minimum level and is technically feasible under following assumptions:

- Thorough quality check of the fingermarks at the level of MS and at the level of CS-SIS, which will guarantee that only "sufficient-quality" fingermarks enter the CS-SIS.
- Fingermarks will be processed by the CS-SIS in a fully lights-out mode.
- This implies that some degree of accuracy will be lost due to unavailability of complementary mark-up introduced by dactyloscopic experts.

Option B: **Adopt a standardized minutia and EFS interchange format**. It is questionable how this a solution would be implemented in practice and how much of a support it would get across the EU MSs' Also, standardizing the EFS closes the doors in theory to future implementation of new technologies, as it is impossible to predict what

kind of features the next generation algorithms are going to use for fingermark / palmmark image comparison. A solution could be the new ISO/IEC 39794-1 and 39794-4 standards, which are forward and backward compatible.

- This solution was likewise adopted in the US. The CJIS division of the FBI enforced the EBTS standard for the interaction with their NGI system (see section 1.7for more details). This standard is derived from the NIST ITL, which is maintained and followed for the inter-agency operations.

Option C: **Use a dedicated interface provided by the future manufacturer of the CS-SIS** for extracting/marking the minutia and extended features which would produce the minutia and EFS vector from the fingermark in a CS-SIS compatible format.

- If the MSs' national ABIS is supplied by different vendor (than that of CS-SIS ABIS), extra investment in terms of effort and resources is to be foreseen at the level of MS to cope with use of "non-standard" equipment[46].

Option D: **Use a dedicated interface developed by a third party** for extracting/marking the minutia and extended features which would produce the minutia and EFS vector in a CS-SIS compatible format.

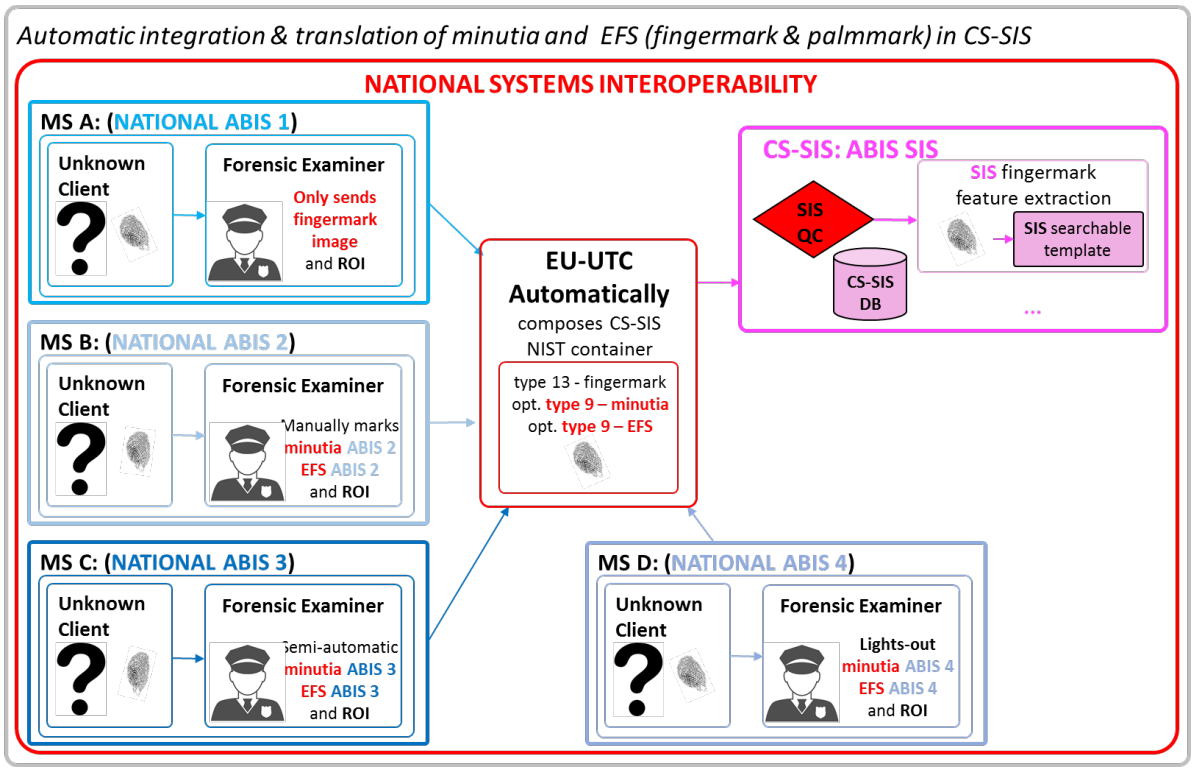
- If the national ABIS is supplied by different vendor (than that of CS-SIS ABIS), extra investment in terms of effort and resources is to be foreseen at the level of MS to cope with use of "non-standard" equipment[47].
- This solution has been adopted in the US, where the FBI commissioned the development and deployment of the Universal Latent Workstation (ULW) for the interaction with their NGI (and former IAFIS).

Option E: **Use a dedicated API plug-in solution** – A European Union Universal Template Converter (EU-UTC) API, which would take as an input the fingermark (or fingermark / palmmark) marked with ROI, minutia and EFS encoded using national ABIS and in a semi-supervised way translates these into a CS-SIS compatible NIST container (depicted in **Figure 18** below).

[46] By the term equipment here we mean additional software and, potentially also different hardware to comply with the requirements of the CS-SIS provider.

[47] By the term equipment here we mean additional software and, potentially also different hardware to comply with the requirements of the CS-SIS provider.

Figure 18. Proposed "create 1, consult all" architecture (Source: EC 2018)



- Two levels of operation could be foreseen – either at the level of MS or at the level of CS-SIS.
- Template compatibility check and fingermark (fingerprint and palmprint) image quality check to be integrated.
- The API would have to be tailor-made to ensure smooth interaction with CS-SIS ABIS.
- This solution is similar to the operation of API provided by the FBI-developed ULW and used in the US for the interaction with the NGI.

Development of the EU-UTC API could be favourable, as it assumes minimum effort at national level and preserves diversity of existing national systems.

Recommendation 20:

Standardized Minutiae and EFS interchange format for the CS-SIS

We recommend adopting for the Central System of SIS a solution in compliance with a standard for Minutiae and EFS interchange format, such as the new ISO/IEC 39794-1 and ISO/IEC39794-4 when become available, as they guarantee forward and backward interoperability.

Standardization process presents several advantages on top of the obvious ones, it:

- Removes possible ambiguities from the public contracts (what is greed upon should be delivered)
- Does not favour any one of the technology providers, and keep healthy competition regarding the performance of the system.

Recommendation 21:

Progressive implementation leading eventually to an EU-Universal Template Converter (EU-UTC)

We recommend in a first stage to allow a fully lights-out mode only (case A together with option A). This first step can be quickly achieved as soon as the future selected fingermark ABIS for the CS-SIS enters into production.

Then in a second step, in order to allow cases B, C and D and to increase accordingly the accuracy of the fingermark ABIS, an EU-UTC API (option E) (which would take as an input a friction ridge image accompanied by the information necessary for creation or consultation of an alert, and automatically produce CS-SIS compliant templates according to the needs/desires of the operator), should be developed and distributed to the MSs in order to be introduced a national level.

Note: the development of this recommendation is based on the cooperation of the vendors providing the necessary modules allowing the conversion as it was successfully achieved by the FBI with the API from its ULW interface.

10. Beyond CS-SIS regulatory framework

10.1. Beyond fingermarks, palmmarks and palmprints

In so far, the present and the 2015 JRC report on the friction ridge impressions has considered use of fingerprints, fingermarks, palmprints and palmmarks. There are however other friction ridge impressions, not covered by the reports.

In the scope of police crime scene investigation, the dactyloscopic examiners often encounter ridge impressions originating from the hypothenar region of the palm (writer's hand) or footprints. Although these biometric samples are not systematically collected, their comparison in the scope of police investigation follows the same principles covered in the former and present reports.

Although in theory, the same feature extraction and comparison algorithms could be used to compare the hypothenar / footprint impressions as for comparing fingerprints / palmprints, given the relatively small-size databases the performance of such systems in terms of rank-1 accuracy in automatic comparisons is still to be validated by further research.

10.2. Bayesian Interpretation Framework

Although the score (comparison score) based biometric systems, such as AFIS, are widely used and adopted across the international spectrum of law enforcement agencies, in the last couple of years, a strong paradigm shift towards adoption of Bayesian Interpretation Frameworks (BIF) and more objective interpretation of Forensic Evidence has emerged. The outcome of a traditional biometric system is a comparison score – a measure of similarity between the probe and reference samples (e.g. fingermark and fingerprint). The paradigm shift observed leans strongly towards reporting the forensic evidence using a BIF in a form of Likelihood Ratios (LRs).

The comparison score on its own is meaningless, therefore a skilled forensic examiner needs to put it in context. Lets' consider the following example – an ABIS-fingermark search returns a comparison score equal to 1500 for a given fingermark-fingerprint pair. Based on this score alone it is impossible to infer the value of the evidence presented, unless we are familiar with the operating parameters of such system, such as:

- Typical low values of comparison scores at the level of non-mated samples (noise)
- Typical high values of comparison scores at the level of mated samples (match)
- Decision threshold (between the match and non-match of an ABIS system)
- Performance characteristics of the system (FMR, FNMR at a given threshold)

The above-mentioned should (and in most cases are) be revealed during the benchmark tests in the call-for-tender, when the performance of to-be-acquired ABIS system gets thoroughly tested on real operational datasets. Despite knowing the above-mentioned operating parameters, the intrinsic evidential value encapsulated within the comparison score is not always obvious or easy to convey. In the majority of the cases the evaluation of such evidence relies on the subjective experience of the forensic practitioner.

In 2015 ENFSI in the scope of the project Strengthening the Evaluation of Forensics Results Across Europe (STEOFRAE) published a guideline for evaluative reporting in

forensic science[48], which provides the forensic practitioners across different disciplines (ridge-based biometrics included) a suggested framework on how to formulate evaluative reports. It recommended the reporting of forensic evidence in a form of LRs, with dedicated examples and use-cases on all biometric modalities. In a BIF, the value of the evidence is determined in the scope of two competing propositions, common nomenclature is a prosecutor (Hp) and defence (Hd):

Hp: The fingermark and the fingerprint originate from the same finger.
Hd: The fingermark and the fingerprint originate from different fingers.

In the simplistic term, the LR can be viewed as a ratio of probabilities of observing given evidence (the event of observing a given comparison score if the fingermark and fingerprint originate from the same finger) under either of the propositions and relevant case-related information:

$$LR = \frac{P(E|Hp, I)}{P(E|Hd, I)}$$

It is not the scope, or a purpose of this report to discuss how the LRs are computed. Many different methods can be found in the forensic literature, which are directly in the domain of fingerprint evidence evaluation [82] [83] [84].

Summary

Expanding the capabilities of the CS-SIS by a Bayesian Interpretation Framework for reporting of forensic evidence has many potential benefits:

- Elimination of the need to "re-evaluate" forensic evidence due to the incompatibility of the matching scores on the side of the consulting MS;
- Immediate integration of the CS-SIS results in subsequent judiciary procedures because decisions at the level of posterior probabilities can be achieved by combining LRs and prior probabilities (domain of the judge);
- Possibility to combine the friction-ridge evidence with other types of evidence at the level of LRs (sometimes referred to as interdisciplinary evidence evaluation);
- More transparent reporting.

[48] http://enfsi.eu/wp-content/uploads/2016/09/m1_guideline.pdf

11. Conclusions

The present study was conducted as a consequence of the new SIS regulatory framework approved in November 2018. In article 33 of the new SIS-Border Regulation and article 43 of the new SIS-Police Regulation, new processing modalities are given to dactyloscopic data stored in SIS alerts:

- Article 33.2 Border checks and Articles 43.2 Police cooperation:

  "Dactyloscopic data may be searched in all cases to identify a person. However, dactyloscopic data shall be searched to identify a person where the identity of the person cannot be ascertained by other means. For that purpose, the Central SIS shall contain an Automated Fingerprint Identification System (AFIS)."

- Article 33.3 Border checks and Article 43.3 Police cooperation:

  "Dactyloscopic data in SIS in relation to alerts entered in accordance with {Articles 24 and 25 for border, Articles 26, 32, 36 and 40 for police} may also be searched using complete or incomplete sets of fingerprints or palm prints discovered at the scenes of serious crimes or terrorist offences under investigation, where it can be established to a high degree of probability that those sets of prints belong to a perpetrator of the offence and provided that the search is carried out simultaneously in the MSs relevant national fingerprints databases."

As a direct consequence of this new Regulation, the objectives defined in Section 1.2 for the study were:

OBJECTIVE 1: Determine the readiness of fingermark, palmmark and palmprint recognition technologies, to be integrated in CS-SIS for the identification of a person.

OBJECTIVE 2: Provide recommendations on the best way to integrate fingermark, palmmark and palmprint recognition technologies in CS-SIS based on: 1) the current state of the art of this technology; 2) the particularities and constraints of CS-SIS and its dual use for law-enforcement and border management.

Given all the information presented in the study, the conclusion reached in the study with respect to the achieved objectives 1 and 2 is that:

CONCLUSION

Given the fact that the large-scale centralized IT systems are successfully deployed at national levels for friction ridge modalities, the present study concludes that:

- ABIS-Fingermark systems have reached a sufficient level of readiness and availability for their integration into SIS, provided that the recommendations listed in the present report are implemented and respected, to the largest extent possible, during the rollout and utilization of the new functionality.

- ABIS-Palmmark and Palmprint systems have reached a sufficient level of readiness and availability for their integration into SIS, provided that the recommendations listed in the present report are implemented and respected, to the largest extent possible, during the rollout and utilization of the new functionality.

Bibliography

[1] A. Jain, K. Nandakumar and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognition Letters,* vol. 79, pp. 80-105, 2016.

[2] A. Jain, A. Ross and S. Pankati, "Biometric: a tool for information security," *IEEE Trans. on Information Forensics and Security,* vol. 1, pp. 125-143, 2006.

[3] C. Champod, C. Lennard, P. Margot and M. Stoilovic, Fingerprints and Other Ridge Skin Impressions, Boca Raton : CRC Press, 2016.

[4] A. Jain, "Automatic Fingerprint Matching Using Extended Feature Set," NIST, 2011.

[5] A. Anthonioz, N. Egli, C. Champod, C. Neumann, R. Puch-Solls and A. Bromage-Griffiths, "Level 3 Details and Their Role in Fingerprint Identification: A Survey among Practitioners," *J. Forensic Identification,* vol. 58, no. 5, pp. 562-589, 2008.

[6] M. Indovina, V. Dvornychenko, R. Hicklin and G. Kiebuzinski, "Evaluation of latent fingerprint technologies: Extended feature sets (evaluation 2)," NIST, NISTIR 7859, 2012.

[7] W. Chapman, A. Hicklin, G. Kiebuzinski, P. Komarinski, J. Mayer-Splain and M. Taylor, "Markup Instructions for Extended Friction Ridge Features," NIST - Special Publication, Washington DC, 2013.

[8] B. Ulery, R. Hicklin, J. Buscaglia and M. Roberts, "Repeatability and reproducibility of decisions by latent fingerprint examiners," *PloS One,* vol. 7, no. 3, 2012.

[9] B. Ulery, R. Hicklin, M. Roberts and R. Buscaglia, "Interexaminer variation of minutia mark-up on latent fingerprints," *Forensic Science International,* vol. 264, pp. 89-99, 2016.

[10] S. Arora, K. Cao, A. Jain and G. Michaud, "Crowd powered latent fingerprint identification: Fusing AFIS with examiner mark-ups," in *International Conference on Biometrics*, Phuket, 2015.

[11] J. Li, J. Feng and C.-C. Jai Kuo, "Deep convolutional neural network for latent fingerprint enhancement," *Signal processing: Image Communication,* vol. 60, pp. 52-63, 2018.

[12] M. Liu, X. Chen and X. Wang, "Latent Fingerprint Enhancement via Multi-Scale Patch Based Sparse Representation," *IEEE Trans. Inf. Forensics Secur.,* vol. 10, no. 1, pp. 6-15, 2015.

[13] J. Zhang, R. Lai and C. Kuo, "Adaptive directional total-variation model for latent fingerprint segmentation," *IEEE Trans. Inf. Forensics Secur.,* vol. 8, no. 8, pp. 1261-1273, 2013.

[14] X. Yang, J. Feng and Z. J., "Localized dictionaries based orientation field estimation for latent fingerprints," *IEEE Trans. Pattern Anal. Mach. Intell.,* vol. 36, no. 5, pp. 955-959, 2014.

[15] K. Cao and A. Jain, "Automated Latent Fingerprint Recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 2018.

[16] R. Labati, A. Genovese, E. Muñoz, V. Piuri and S. F., "A novel pore extraction method for heterogeneous fingerprint images using Convolutional Neural Networks," *Pattern Recognition Letters,* vol. 000, pp. 1-9, 2017.

[17] W. Lee, S. Cho, H. Choi and K. J., "Partial fingerprint matching using minutiae and ridge shape features for small fingerprint scanners," *Expert Systems With Applications,* vol. 87, pp. 183-198, 2017.

[18] S. Mathur, A. Vjay, J. Shah, S. Das and A. Malla, "Methodology for partial fingerprint enrollment and authentication on mobile devices," in *International Conference on Biometrics*, Halmstad, 2016.

[19] S. Liu, M. M. Liu and Z. Yang, "Sparse coding based orientation estimation for latent fingerprints," *Pattern Recognition,* vol. 67, pp. 164-176, 2017.

[20] S. Chikkerur, A. A.N. Cartwright and V. Govindaraju, "Fingerprint enhancement using STFT analysis," *Pattern Recognition,* vol. 40, no. 1, pp. 198-211, 2007.

[21] Y. Wang, J. J. Hu and D. Phillips, " fingerprint orientation model based on 2d fourier expansion (FOMFE) and its application to singular-point detection and fingerprint indexing," *EEE Trans. Pattern Anal. Mach. Intell.,* vol. 29, no. 4, pp. 573-585, 2007.

[22] J. Feng, J. Zhou and J. A.K., "Orientation field estimation for latent fingerprint enhancement," *IEEE Trans. Pattern Anal. Mach. Intell.,* vol. 35, no. 4, pp. 925-940, 2013.

[23] X. Yang, J. Feng and J. Zhou, "Localized dictionaries based orientation field estimation for latent fingerprints," *IEEE Trans. Pattern Anal. Mach. Intell.,* vol. 36, no. 5, pp. 955-969, 2014.

[24] R. Krish, J. Fierrez, D. Ramos, F. Alonso-Fernandez and J. Bigun, "mproving automated latent fingerprint identification using extended minutia types," *Information Fusion,* vol. 50, pp. 9-19, 2019.

[25] M. Indovina, H. R.A. and K. G.I., "ELFT-EFS. Evaluation of Latent Fingerprint Technologies: Extended Feature Sets," NIST, NISTIR 7775, 2011.

[26] V. Dvornychenko and M. Garris, "Summary of NIST latent fingerprint testing workshop," NIST, NISTIR 7377, 2006.

[27] M. Indovina, V. Dvornychenko, E. Tabassi, G. Quinn, P. Grother, S. Meagher and G. M., "ELFT Phase II - An Evaluation of Automated Latent Fingerprint Identification Technologies," NIST, NISTIR 7577, 2009.

[28] C. J., "Best practices and time utilization in searching local, state and federal AFIS," FBI, 2013.

[29] C. Watson, G. Fiumara, E. Tabassi, S. Cheng, P. Flanagan and W. Salamon, "Fingerprint Vendor Technology Evaluation," NIST, NISTIR 8034, 2014.

[30] Office of the Inspector General, "A Review of the FBI's Handling of the Brandon Mayfield Case," US Department of Justice, Washington, D.C., 2016.

[31] B. Budowle, J. Buscaglia and R. Perlman, "Review of the scientific basis for friction ridge comparisons as a means of identification: Committee findings and recommendations," *Forensic Sci Commun,* vol. 8, no. 1, 2006.

[32] National Research Council, " Strengthening Forensic Science in the United States: A Path Forward," National Academies Press, Washington D.C., 2009.

[33] K. J.J., "Fingerprint error rates and proficiency tests: What they are and why they matter," *Hastings Law J,* vol. 59, pp. 1077-1110, 2008.

[34] J. Mnookin, "The validity of latent fingerprint identification: Confessions of a fingerprinting moderate," *Law Probability and Risk,* vol. 7, pp. 127-141, 2008.

[35] B. Ulery, R. Hicklin, J. Buscaglia and M. Roberts, "Accuracy and reliability of forensic latent fingerprint decisions," in *Proceedings of the National Academy of Sciences of the United States of America*, 2011.

[36] P. C. a. A. o. S. a. Technology, "Report to the President of Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods," Executive Office of the President, Washington DC, 2016.

[37] W. Thompson, J. Black, A. Jain and J. Kadane, "Forensic Science Assessment - a Quality and Gap Analysis - new Ways of Reporting Fingerprint Evidence," American Association for the Advancement of Science, Washington DC, 2017.

[38] T. Chung, K. Cao, E. Tabassi and A. Jain, "Latent Fingerprint Value Prediction: Crowd-based Learning," *IEEE Transactions on Information Forensics and Security,* 2018.

[39] National Institute of Justice, The Fingerprint Sourcebook, U.S. Department of Justice, 2002.

[40] A. Gumaei, R. Sammouda, A. Al-Salman and A. Alsanad, "An Improved Multispectral Palmprint Recognition System Using Autoencoder with Regularized Extreme Learning Machine," *Computational Intelligence and Neuroscience,* vol. 2018, 2018.

[41] X. Xu, Z. Guo, C. Song and Y. Li, "Multispectral palmprint recognition using a quaternion matrix," *Sensors,* vol. 12, no. 4, p. 4633–4647, 2012.

[42] J. Haryati, I. Salwani and D. A.R., "A Robust and Fast Computation Touchless Palm Print Recognition System Using LHEAT and the IFkNCN Classifier," *Computational Intelligence and Neuroscience,* vol. 2015, no. 17, 2015.

[43] D. Zhang, Z. Guo, G. Lu, L. Zhang and W. Zuo, "An online system of multispectral palmprint verification," *IEEE Transactions on Instrumentation and Measurement,* vol. 59, no. 2, pp. 480-490, 2010.

[44] X. Xu, T. Lu, X. Zhang, H. Lu and W. Deng, "Multispectral palmprint recognition using multiclass projection extreme learning machine and digital shearlet transform," *Neural Computing and Applications,* vol. 27, no. 1, pp. 143-153, 2016.

[45] L. Lu, X. Zhang, X. Xu and D. Shang, "Multispectral image fusion for illumination-invariant palmprint recognition," *PLoS ONE,* vol. 12, no. 5, 2017.

[46] A. El-Tarhouni, L. Boubchir, N. Al-Maadeed, M. Elbendak and A. Bouridane, "Multispectral palmprint recognition based on local binary pattern histogram fourier features and gabor filter," in *6th European Workshop on Visual Information Processing (EUVIP)*, Marseille, 2016.

[47] M. Bounneche, L. Boubchir, A. Bouridane, B. Nekhoula and A. Ali-Chérif., "Multi-spectral palmprint recognition based on oriented multiscale log-Gabor filters," *Neurocomputing,* vol. 205, pp. 274-286, 2016.

[48] D. Hong, W. Liu, J. Su, Z. Pan and G. Wang, "A novel hierarchical approach for multispectral palmprint recognition," *Neurocomputing,* vol. 151, no. 1, pp. 511-521, 2015.

[49] M. Arunkumar and S. Valarmathy, "Palm Print Identification Using Improved Histogram of Oriented Lines," *Circuits and Systems,* vol. 07, pp. 1665-1676, 2016.

[50] S. Lin, Y. Wang, T. Xu and Y. Tang, "Palmprint and Palm Vein Multimodal Fusion Biometrics Based on MMNBP," in *Chinese Conference on Biometric Recognition (CCBR)*, Chengdu, 2016.

[51] P. Li, Z. Miao and Z. Wang, "Fusion of palmprint and palm vein images for person recognition," in *International Conference on Signal Processing (ICSP)*, Hangzhou, 2014.

[52] E. Liu, A. Jain and J. Tian, "A coarse to fine minutiae-based latent palmprint matching," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 35, no. 10, pp. 2307-2322, 2013.

[53] Y. Zheng, Y. Liu, G. Shi, J. Li and Q. Wang, "Segmentation of offline palmprint," in *Third International IEEE Conference on Signal-Image Technologies and Internet-Based System*, Shanghai, 2007.

[54] Y. Zheng, G. Shi, L. Zhang, Q. Wang and Z. YJ., "Research on offline palmprint image enhancement," in *IEEE International Conference on Image Processing*, San Antonio, TX, 2007.

[55] J. Li and G. Shi, "A novel palmprint feature processing method based on skeleton image," in *IEEE International Conference on Signal Image Technology and Internet Based Systems (SITIS'08)*, Bali, 2008.

[56] J. Li, G. Shi, Y. Zheng and Y. Liu, "The research on offline palmprint identification," in *IEEE World Congress on Computer Science and Information Engineering (CSIE'09)*, Los Angeles, CA, 2009.

[57] J. Yang, G. Shi, S. Chang, Z. Tan and Z. Shang, "A novel method of minutiae filtering based on line feature extraction," in *IEEE International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC'09)*, Hangzhou, 2009.

[58] Z. Tan, J. Yang, Z. Shang, G. Shi and S. Chang, "Minutiae-based offline palmprint identification system," in *WRI Global Congress on Intelligent Systems*, Xiamen, 2009.

[59] A. Jain and J. Feng, "On latent palmprint matching," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 31, no. 6, pp. 1032-1047, 2009.

[60] R. Cappelli, M. Ferrara and D. Maio, "A fast and accurate palmprint recognition system based on minutiae," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics),* vol. 42, no. 3, pp. 956-962, 2012.

[61] J. Dai and J. Zhou, "Multifeature-based high-resolution palmprint recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 33, no. 5, pp. 945-957, 2011.

[62] J. Dai, J. Feng and J. Zhou, "Robust and efficient ridge-based palmprint matching," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 34, no. 8, pp. 1618-1632, 2012.

[63] M. Aguado-Martínez and J. Hernández-Palancar, "Speeding up High Resolution Palmprint Matching by Using Singular Points," in *Progress in Artificial Intelligence and Pattern Recognition*, Lecture Notes in Computer Science (IWAIPR 2018), 2018.

[64] A. Jain and J. Feng, "Latent palmprint matching," *IEEE Trans. on Pattern Analysis and Machine Intelligence,* vol. 31, no. 6, pp. 1032-1047, 2009.

[65] R. Wang, D. Ramos and J. Fierrez, "Latent-to-full palmprint comparison based on radial triangulation under forensic conditions," in *International Joint Conference on Biometrics (IJCB)*, Washington, D.C., 2011.

[66] R. Wang, D. Ramos, R. Veldhuis, J. Fierrez, L. Spreeuwers and H. Xu, "Regional fusion for high-resolution palmprint recognition using spectral minutiae representation," *IET Biometrics,* vol. 3, no. 2, pp. 94-100, 2014.

[67] A. Morales, M. Medina-Pérez, M. Ferrer, M. García-Borroto and R. L.A., "LPIDB v1.0 - Latent palmprint identification database," in *IEEE International Joint Conference on Biometrics*, Clearwater, FL, 2014.

[68] J. Dai, J. Feng and J. Zhou, "Robust and efficient ridge-based palmprint matching," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 34, no. 8, p. 2012, 2011.

[69] F. Alonso-Fernandez, J. Fierrez and J. Ortega-Garcia, "Quality Measures in Biometric Systems," *IEEE Security & Privacy,* vol. 10, pp. 52-62, 2012.

[70] E. Tabassi, C. L. Wilson and C. I. Watson, "Fingerprint Image Quality," NISTIR 7151, 2004.

[71] P. Grother and E. Tabassi, "Performance of Biometric Quality Measures," *IEEE Trans. Pattern Analysis and Machine Intelligence,* vol. 29, pp. 531-543, 2007.

[72] Latent Print Services, FBI, "Universal Latent Workstation v_6.6.7," 2018. [Online]. Available: https://www.fbibiospecs.cjis.gov/Latent/PrintServices. [Accessed 10 12 2018].

[73] H. Hicklin, J. Buscaglia and R. M.A., "Assessing the Clarity of Friction Ridge Impressions," *Forensic Science International,* vol. 226, pp. 106-117, 2013.

[74] S. Yoon, E. Liu and A. Jain, "On Latent Fingerprint Image Quality," in *International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, Arlington, VA, 2013.

[75] S. Yoon, E. Liu and A. Jain, "On Latent Fingerprint Image Quality," in *International Workshop on Computational Forensics*, Jakuba, 2012.

[76] S. Yoon, E. Liu and A. Jain, "On Latent Fingerprint Image Quality," in *International Workshop on Computational Forensics*, Stockholm, 2014.

[77] L. Beslay, J. Galbally-Herrero and J. Nordvik, "Fingerprint identification technology for its implementation in the Schengen Information System II (SIS-II)," Publications Office of the European Union, 2015.

[78] E. Tabassi, "Development of NFIQ 2.0," NIST, 2014. [Online]. Available: https://www.nist.gov/services-resources/software/development-nfiq-20. [Accessed 10 12 2018].

[79] E. Tabassi, M. Olsen, M. A. and C. Busch, "Towards NFIQ II Lite, NIST Interagency report 7973," NIST, Washington DC, 2013.

[80] K. Han, R. Ma and X. Jing, "A new method for tenprint image quality evaluation," in *IMCEC 2018*, Xi\'an, 2018.

[81] F. Hao, L. Yang, G. Yang, N. Liu and Z. Liu, "RFPIQM: Ridge-Based Forensic Palmprint Image Quality Measurement," *IEEE Access,* vol. 6, pp. 62076-62088, 2018.

[82] C. Neumann, C. Champod, R. Puch-Solis, N. Egli, A. Anthonioz and A. Bromage-Griffiths, "Computation of likelihood ratios in fingerprint identification for configurations of any number of minutiae.," *Journal of Forensic Sciences,* vol. 52, no. 1, pp. 54-64, 2017.

[83] N. Egli, *Interpretation of partial fingermarks using an automated fingerprint identification system,* PhD thesis, University of Lausanne, 2009.

[84] R. Haraksim, D. Ramos and D. Meuwly, "Validation of likelihood ratio methods for forensic evidence evaluation handling multimodal score distributions," *IET Biometrics,* vol. 6, no. 2, pp. 61-69, 2017.

Annex 1: Comparison table of Prüm and CS-SIS

Aspect	Prüm	CS-SIS (AFIS)
Availability	24/7 but only maximum response time of 24 hours is guaranteed. Could be faster at certain times.	24/7, no restriction. Response time may only be limited by the available resources of the central data base[49].
Accessibility	In the course of individual investigation cases.	Only "administrative" purposes are excluded. All other purposes must be in accordance with individual national law.
Real-time Access	Not possible because of the 24 hours constraint.	Although the term real-time is relative, current response time of SIS-AFIS is within 7 seconds.
Accuracy	Individual response depends on the national AFIS and its configuration. No uniform thresholds whatsoever.	Detailed statistics are yet to be made available following the March 2018 roll-out.
Data size	Joint AFIS data of all connected countries, presumably in the range of tens of millions of persons.	In 2017 there were roughly 900K person-related alerts stored in CS-SIS.
Degree of automation	Queries can be generated quite conveniently but response in each queried country needs to be triggered manually.	Interface and response are comparable with a state-of-the-art AFIS systems.
Level of received information	Only hit lists and an anonymized reference number. No links to potential national or international alerts. Fingerprints can only be displayed but not retrieved. Additional information about certain hits needs to be requested via channels not specified in the Council Decision and with no time frame specification.	All information attached by the MS who has issued the alert in SIS II, including full access to the relevant fingerprint data. More information can be requested from national SIRENE offices but without time frame specification.

[49] To quantify the needs is subject of this study.

Annex 2: Outline of Technical meeting with MSs national experts for fingermark recognition discussion

EUROPEAN COMMISSION
DIRECTORATE GENERAL JRC
JOINT RESEARCH CENTRE
Directorate E - Space, Security and Migration
Cyber and Digital Citizens' Security Unit – Unit E.03

JRC study on latent and face recognition technologies for their introduction in the SIS central.

Outline of Technical meeting with national Fingermark Experts

USE CASES SIS II AFIS-Fingermark

What is the most typical query / use case you are planning to submit to the SIS II AFIS in case of fingermark?
For each type of request:

- Format to be used
- Expected response time
- Type of response: single answer or ranked list
- Acceptable performance with respect to accuracy
- Type of data involved

How would the MS proceed upon reception of a positive SIS II AFIS response?

NATIONAL AFIS SYSTEM

What kind of national AFIS system is implemented? (Vendor + version)
Does the MS have a dedicated fingermark database?
What kind of preparatory processing operations are needed in a search with fingermarks?
What type of templates are involved? Are they compatible with ISO standards or other standards?
Is quality check performed on the fingermarks prior to their enrolment in the database AFIS?

What are the differences between the 10-print AFIS and the fingermark AFIS (same engine, same server, procedure)?
How MS interacts with the national AFIS? (e.g. 1:N search / 10print:10print search / fingermark:N search / fingermark:10print search / Fingermark : Fingermark)
Are the **unresolved** fingermarks stored?

- If so, what procedure is followed?
- If so, in what format?
- If so, how many unresolved fingermarks does the MS have on record in 2017– what is the size of the unresolved fingermark database?
- If **not**, what happens to the unresolved fingermark?

Was the national AFIS subject to a benchmark (fingermark) test?
Does the national AFIS run in the "lights-out" mode with fingermarks?
What search filters does the AFIS have? For instance:

- Date
- Type (flat, rolled, fingermark…)
- Origin (country)
- Fingerprint class (right loop, left loop, whorl…)
- Quality

HUMAN INTERVENTION

Are fingerprints and fingermarks being processed according to the ACEV (Acquisition, Comparison, Evaluation, Verification) procedure?

Are human operators involved in processing of fingermarks prior to their enrolment in the AFIS system?

- If so, to what extent (e.g. manual feature extraction / automatic feature extraction + manual verification / quality etc.)

QUALITY

Is quality of the fingermarks verified?

- If so, in what stage of the ACEV procedure?
- If so, what quality metric is used?
- If so, is the quality metric propagated with the fingerprint, fingermark all the way through the ACEV process?
- If so, is the quality metric being **actively** used to determine the usability of the fingermark in the AFIS search?

DATA

Do MSs have a centralized database or are the data otherwise organized?

How were fingerprints obtained? What experience exists on interoperability of data obtained by different methodologies?

Statistics on quality of data? Is there a quality threshold?

Is there a minimum number of minutiae for a fingermark to be stored?

Is data flagged according to its type/quality/origin?

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696, or
- by electronic mail via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from EU Bookshop at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

KJ-NA-29755-EN-N

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi:10.2760/852462

ISBN 978-92-76-03975-4