



JRC SCIENCE FOR POLICY REPORT

An AFIS functionality for the European Criminal Records Information System

A preliminary assessment of DG JUST decentralised option supported by pseudonymised index-filter

Beslay, L
Galbally, J

2016



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: Via E.Fermi 2749-I-21027 ISPRA (VA) - Italy
E-mail: laurent.beslay@ec.europa.eu
Tel.: +39-0332-786.55.6

JRC Science Hub

<https://ec.europa.eu/jrc>

JRC102773

EUR 28075 EN

PDF ISBN 978-92-79-61299-2 ISSN 1831-9424 doi:10.2788/26312

Luxembourg: Publications Office of the European Union, 2016

© European Union, 2016

The reuse of the document is authorised, provided the source is acknowledged and the original meaning or message of the texts are not distorted. The European Commission shall not be held liable for any consequences stemming from the reuse.

How to cite this report: Laurent Beslay and Javier Galbally, *An AFIS functionality for the European Criminal Records Information System*, EUR 28075 EN, doi:10.2788/26312

All images © European Union 2016,

Title: An AFIS functionality for the European Criminal Records Information System

Abstract

At the request of DG JUST, the JRC presents in this background note a preliminary assessment of a possible successful introduction of a new Automatic Fingerprint Identification System (AFIS) functionality in ECRIS. It provides a technical assessment of the proposed decentralized privacy-preserving approach based on a pseudonymised index-filter shared by all Member States (MS), and lists the main technical and architectural challenges.

Contents

Foreword.....	2
1 Scene setter: An AFIS for addressing new challenges	3
2 Privacy by design for Biometric Systems	5
2.1 Privacy challenges in Biometric Systems	5
2.1.1 General biometric privacy challenges	5
2.1.2 Biometric privacy challenges in the context of ECRIS	6
2.2 Properties to be assessed in Biometric Privacy Preserving Systems	7
2.3 Biometric Template Protection (BTP) approaches.....	8
2.3.1 Research state-of-play	8
2.3.2 A BTP case study: TURBINE FP7 project.	8
3 Challenges of integrating an AFIS in a decentralized ECRIS architecture.....	10
3.1 Acquisition scanner.....	10
3.2 Feature Extractor and Matcher	10
3.3 Quality metric algorithm(s).....	11
3.4 Other architectural considerations	12
3.4.1 Type of fingerprint data to be stored in the index-filter.....	12
3.4.2 Unique or separate indexes for alpha-numeric and fingerprint data.....	13
3.4.3 Unique or separate entries for TCN convicted in different MS.	16
4 Conclusions and Recommendations	18

Foreword

The European Criminal Records Information System (ECRIS) is a system that aims at exchanging criminal records information among the 28 EU Member States through the s-TESTA network in an electronic way, so that previous convictions in another Member State (MS) can be taken into account at the time of a new conviction.

Delivered in February 2016, the present background note has been produced in the framework of the initial round of consultations undertaken by DG JUST in order to assess the conditions for a successful introduction of a new Automatic Fingerprint Identification System (AFIS) functionality in ECRIS. The objective of this ECRIS update is to cope with the challenges raised by the management of Third Country Nationals (TCN) criminal records.

DG JUST has already suggested an initial proposal for the integration of an AFIS within ECRIS following a decentralized privacy-preserving approach that is based on a pseudonymised index-filter shared by all Member States (MS).

In view of this initial proposal, the Joint Research Centre (JRC) through its Institute for the Protection and Security of the Citizen (IPSC), has been preliminary consulted in order to give an early opinion regarding its feasibility.

The note presents:

1. a technical assessment regarding the proposed solution for the integration of an AFIS in ECRIS;
2. a list of the main technical and architectural challenges which need to be carefully addressed in the development of a feasible solution for the integration of an AFIS in ECRIS.

The note should not be understood as a detailed final study but rather as a first input built upon the JRC: 1) extensive knowledge of other European large AFIS systems already operational; 2) significant background expertise in biometrics and specifically on privacy preserving algorithms for biometric systems.

For sake of clarity, the conclusion of the assessment regarding the proposed solution is already presented here below:

OVERALL ASSESSMENT

The current proposal for the inclusion of an AFIS within ECRIS, based on a decentralized architecture with a pseudonymised index-filter shared by all MS, presents severe flaws that will most likely lead to a failure of the fingerprint-based search engine.

The pseudonymised dimension of the index-filter has been identified as the element of the proposal that will jeopardize the performance of the envisaged system new AFIS.

This statement is further elaborated and justified within the document.

1 Scene setter: An AFIS for addressing new challenges

When a Member State A is convicting an EU National from a Member State B, the identification of this Member State B is usually straightforward. ECRIS offers then the possibility for Member State A to obtain the possible criminal records of this EU National from Member State B.

In the case of a Third Country National (TCN), Member state A will have to send a request to all the other MSs using potentially less reliable information. As such, TCNs represent today a double challenge for ECRIS users:

1. Their correct identification is difficult due to absence of ID document and/or documents which do not offer an equivalent level of security as the ones from EU nationals.
2. Unless solid contextual information is available, it is usually impossible to identify the Member State(s) already holding criminal record information on a TCN.

In order to address these two challenges, it has been proposed to use:

- **the fingerprints of the TCN**, i.e., an identifier which is available most of the time even in absence of any ID document:, and
- **an index-filter**, i.e., a system providing a link between this identifier and the Member State that holds the related criminal records.

The use of an Automatic Fingerprint Identification System (AFIS) is clearly a solid option for addressing successfully the challenges listed above. As it has been already demonstrated¹, the readiness and availability of AFIS technology have reached a mature and satisfactory level for its deployment in large scale IT systems such as EURODAC, the Visa Information System (VIS) or more recently the Schengen Information System II (SIS-II). Regarding SIS-II, Member States recognized that the very limited number of fingerprints already stored in the database (although allowed since May 2013) was mainly due to the absence of an AFIS functionally which will permit a reliable identification of data subjects with no ID document.

The 2014 figures provided by EURODAC, represent an interesting input for the future development of ECRIS as the goal, the technical characteristics and volume could be seen as quite similar. In EURODAC the goal is to identify the Member State which dealt first with an asylum seeker using few personal data from the data subject and in particular his/her fingerprint information in the form of a ten print card². According to the Annual Report 2014 produced by eu-LISA, EURODAC stores 2.7 million sets of fingerprints (ten prints flat) and a total of 756,368 transactions took place. The fingerprint rejection rate observed in 2014 was 4.49%.

It should be underlined however that EURODAC presents some significant architectural differences with respect to the proposed solution for ECRIS, namely:

1. EURODAC is a centralised system relying on a single database;
2. it is equipped with a single matching system;
3. the matching process is performed on non-protected (i.e., non-anonymized) fingerprint templates.

¹ <http://publications.jrc.ec.europa.eu/repository/handle/JRC97779>

² See article 11 of EURODAC Regulation (EU) No 603/2013 <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0603&from=FR>

Given the discussion above, the main conclusion that may be reached is:

RECOMMENDATION 1.

The inclusion of an AFIS within ECRIS seems to be the most suitable solution (and possibly also the only solution) to deal with the challenges that TCN currently pose to the ECRIS system.

However, given the architecture currently proposed for ECRIS, the integration of an AFIS is not straight forward and should be the topic of a dedicated study. Two main characteristics stand out at the moment in the architecture of ECRIS:

1. Possible **pseudonymised** index-filter, following the application of privacy by design principle.
2. **Decentralized** system.

These two characteristics trigger certain challenges for the integration of an AFIS that will be introduced in Sects. 2 and 3.

2 Privacy by design for Biometric Systems

NOTE: The most relevant biometric related terms used in the following sections are defined in Annex A.

Several questions should be addressed when dealing with the protection of biometric information in order to preserve the user's privacy and data protection rights. Depending on the scenario considered it is possible that not all the privacy challenges presented in this section are necessarily applicable. For instance, the privacy level required for a civil biometric system such as EURODAC or the VIS may not be the same as the privacy level required for a criminal application such as ECRIS or SIS-II.

Privacy challenges may vary as well between verification (a 1-to-1 comparison) and identification systems (a 1-to-*N* comparison such as an AFIS). However, for the sake of completeness, all the most common privacy issues related to biometric systems are enumerated in section 2.1.

The aim of the present document is not to conduct a Privacy Impact Assessment on ECRIS but only to explore those most common privacy challenges and assess their relevance in the context of this system. For a more exhaustive approach the reader is invited to go through the opinions adopted by the Article 29 of the data protection Working Party on biometric topics (mainly WP193 and WP80)³.

2.1 Privacy challenges in Biometric Systems

2.1.1 General biometric privacy challenges

- **PRIVACY CHALLENGE 1: INVERSE BIOMETRICS.** *Do the stored templates reveal any information about the original biometric samples? In other words, are we able to reconstruct synthetic samples whose templates are similar enough to those of the original subject? For such an inverse engineering process, an eventual attacker which manages to obtain just a template belonging to a certain subject (e.g. minutiae template) would be able to reconstruct the original biometric sample. The attacker could afterwards use it to illegally access the system or even to steal someone's identity, thus violating privacy and data protection rights of the data subject. Although technically possible, a successful inverse engineering process is really difficult to achieve and rely usually on favorable laboratory conditions with for example template proposing a very high number of minutiae.*
- **PRIVACY CHALLENGE 2: CROSS-MATCHING.** *Are my enrolled templates in different recognition systems somehow related to each other? Can someone cross-match those templates and track my activities? With the widespread use of biometrics in many everyday tasks, a particular subject will probably enroll in different applications, such as health care or on-line banking, with the same biometric characteristic. An eventual attacker who gets access to the same template enrolled in different biometric systems could combine that information and build detailed profiles of an individual's behavior. Therefore, cross-matching between templates used in different applications should be prevented.*
- **PRIVACY CHALLENGE 3: IRREVOCABILITY.** *What if someone steals a template extracted from my right index finger? Won't I be able to use that finger again to enroll into the system? Has it been permanently compromised? Since biometric characteristics are unique and permanent (it cannot be replaced), it should be possible to generate multiple templates from this single biometric characteristic in order to discard and replace compromised templates. Furthermore, those*

³ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

templates should not be related to one another, in the sense that they should not be positively matched by the biometric system, to prevent the impersonation of a subject with a stolen template. Consequently, renewability of biometric templates is also desired whenever possible.

2.1.2 Biometric privacy challenges in the context of ECRIS

Without conducting a full and exhaustive threat analysis, two main threats can be considered already at this stage:

1. Access and misuse of the fingerprint data from a third party.
2. Abuse of the fingerprint data from an ECRIS user (i.e., Member State).

If the objective of the foreseen privacy safeguards is to protect the data from third parties (possible data leak to third parties from *outside* ECRIS), then it should be analysed if it is relevant to adopt greater protection measures in ECRIS than in the individual national systems from which data will be sent to ECRIS. In other words, even if ECRIS would benefit from a complete protection, a third party could always try to access the data at the initial national systems as the weakest link of the security chain.

Should the objective of the privacy safeguards be to protect the fingerprint data among the ECRIS users, then several observations can be made regarding the biometric privacy challenges listed above:

- **INVERSE BIOMETRICS in the case of ECRIS.** The relevance of this issue is rather low from a procedural and environmental point of view. In case of a hit, the MS might want to have access to the fingerprint image stored in order to confirm the result by manually comparing it with the one submitted (as it is the case in EURODAC). This will imply that not only the template but also the image will eventually be available to the Member State. This way, Member State A will not need to turn to an inverse biometrics attack in order to have access to the fingerprint images of Member State B.
- **CROSS MATCHING in the case of ECRIS.** To a certain extent the purpose of ECRIS is exactly to conduct cross-matching and find if the convicted TCN has not been registered/arrested already in another Member State. It has to be underlined as well that the log files generated for each access and the very strict access control policy will already greatly mitigate this potential risk.
- **IRREVOCABILITY in the case of ECRIS.** This last issue is in general not applicable to ECRIS which is not an access control system based on biometrics (such as the one of a sport club or a bank).

RECOMMENDATION 2.

The most appropriate way to address potential privacy challenges in the context of ECRIS is to conduct a Data Protection Impact Assessment which will identify and quantify the risks related to the system in production and to evaluate the appropriateness of the security measures foreseen. Undermining privacy risks will have the same negative effect as overshooting them.

A good starting point is to assess the security measures and data protection requirements already applied to similar national criminal systems or at least such as EURODAC.

2.2 Properties to be assessed in Biometric Privacy Preserving Systems

In order to address the previous potential privacy challenges and in case they might be relevant in the context of ECRIS, according to the standard ISO/IEC IS 24745 [ISO/IEC 2011], the next two properties should be guaranteed:

- **Irreversibility:** in order to overcome the first privacy challenge (i.e., amount of biometric information which is leaked by the template), it is required that knowledge of a protected template cannot be exploited to reconstruct a “synthetic” biometric signal which positively matches the original biometric sample. This property prevents the abuse of stored biometric data for launching spoof or replay attacks, thereby improving the security of biometric systems.
- **Unlinkability:** in order to overcome the second and third privacy challenges of unprotected biometric systems (i.e., biometric characteristics should not be matched across systems and they should be revocable), given a single biometric sample, it must be feasible to generate different versions of protected templates, so that those templates cannot be linked to a single subject. This property guarantees the privacy of a subject when he is registered in different applications with the same biometric characteristic (prevents cross-matching), and also allows issuing new credentials in case a protected template is stolen.

In addition to the irreversibility and unlinkability properties mentioned in the ISO standard, in order to consider biometric template protection approach as a viable solution, the following two principles related to performance parameters need to be respected:

- **Accuracy:** protected biometric systems that enhance user’s privacy (i.e., meet the irreversibility and unlinkability requirements) should present a recognition accuracy which is comparable to the one obtained by standard un-protected systems. This parameter is especially relevant for a large IT system such as ECRIS, where Member States will expect the accuracy of the AFIS functionality to be at least equivalent to the one of their own national criminal AFIS.
- **Computational processing:** usually the extra processing required to generate and match protected biometric templates brings a significant computational burden that slows down the system. The final speed can be a very important parameter especially in large IT systems such as ECRIS. The possible impact of such additional processing should therefore be assessed.

RECOMMENDATION 3.

We recommend to carefully assess to which extent irreversibility, unlinkability, accuracy and speed are required for the implementation of an AFIS in ECRIS:

- Should irreversibility be granted?
- Should unlinkability be granted?
- What is the expected minimum accuracy of the AFIS (at least equivalent to those national ones)?
- What is the expected speed of the AFIS (at least equivalent to those national ones)?

2.3 Biometric Template Protection (BTP) approaches

NOTE: The reader should bear in mind that the following discussion affects only the case in which the matching of biometric samples is carried out in the protected domain.

2.3.1 Research state-of-play

When applied on alpha-numeric data, *standard privacy safeguards* offer very satisfactory results (i.e., they comply to a high extent with the properties presented in Sect. 2.2). However, extensive tests carried out over the last 10 years have shown that such techniques fail to give an acceptable accuracy level when they are directly applied to biometric data. For this reason, the research community has developed new privacy preserving algorithms adapted to the specificities of the biometric technology. All that research effort is encompassed in a field referred to as *Biometric Template Protection (BTP)* [Nandakumar and Jain 2015].

A good review of the state of the art in BTP may be found in [Campisi, 2013; Rathgeb and Uhl, 2011]. Usually BTP algorithms are classified in three main categories:

- **Cancelable biometrics.** These algorithms consist of intentional, repeatable distortions of biometric signals based on transformations which provide a comparison of biometric templates in the protected domain [Ratha et al., 2001]. There are two main types of cancelable biometric schemes: 1) *Non-reversible transformations* of the biometric data or unprotected templates [Ratha et al. 2007, Boulton, 2006, Rathgeb et al., 2013a,b]; 2) *Biometric salting*, in which auxiliary data is blended with biometric data to derive a distorted version of the biometric sample [Teoh et al., 2006, Pillai et al., 2011].
- **Cryptobiometrics.** These methods combine cryptographic keys with transformed versions of the original biometric templates to obtain secure templates. In most cases, some public information, known as helper data or auxiliary data (AD), is generated. Depending on how the AD is used, cryptobiometric schemes can be broadly divided into: 1) *Key binding schemes*, where AD are obtained combining the key with the biometric template. At verification time, applying an appropriate key retrieval algorithm to the probe biometric sample, the key is obtained from the AD. Most of these techniques are based on the fuzzy vault and the fuzzy commitment schemes [Nandakumar 2010, Nandakumar et al. 2007]. 2) *Key generation schemes*, where both the AD and the key are generated directly from biometric data. Again, at verification time, a key is recovered from the probe sample using the AD [Vielhauer et al. 2002, Teoh et al. 2004].
- **Biometrics in the encrypted domain.** As an alternative to the aforementioned methods based on cancelable biometrics or cryptobiometrics, *Homomorphic Encryption* schemes allow for computations to be performed on ciphertexts, with no additional AD, and which generate encrypted results which decrypt to plaintexts that match the result of the operations carried out on the original plaintext. Since practical implementations of Fully Homomorphic Encryption (FHE) schemes still remain a big challenge, semi Homomorphic Encryption (HE) schemes, which only allow a limited subset of operations in the encrypted domain, are nowadays being introduced into biometrics [Barni et al., 2010; Bringer et al., 2013; Ye et al., 2009].

2.3.2 A BTP case study: TURBINE FP7 project.

In addition to the different references to research in the BTP field given in section 2.3, a good practical example of the results that can be expected from BTP algorithms is the EU FP7 project "TURBINE: Trusted Revocable Biometrics Identities". The two main goals of TURBINE were:

- to develop an innovative, privacy enhancing technology solution for electronic identity (eID) authentication through fingerprints biometrics, and
- to demonstrate the performance and security of this solution for use in commercial eID management applications as well as its benefit for the citizen in terms of enhanced privacy protection and user trust in electronic identity management through the use of fingerprints.

The algorithms for trusted and revocable biometric identities were tested and evaluated in two testing rounds. Performance tests were conducted both at the minutiae (unprotected) and at the pseudo-identity (protected) levels. All the tests were carried out independently using the GUC100 fingerprint database as a primary test database of the project which consists of 100 data subjects and the use of 6 scanners (a total of 72000 fingerprint images were produced). The algorithm suppliers did not have access to the GUC100 database. The target performance of the project was specified in the beginning of the project as (lower or) 1% False Rejection Rate at 0.1% False Acceptance Rate.

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

The overall conclusion of the TURBINE project after the tests was that: it would be quite challenging to achieve the project's target performance, especially at the pseudo identity (protected) level.

The TURBINE project ended in 2011 and several promising advances have been achieved since then in the field of BTP (as presented in Sect. 2.3.1.) However, none of the new techniques proposed so far have been tested on large IT systems in production and all evidence collected from the state of the art leads to think that there is still a significant gap in the performance of biometric systems between the unprotected and the protected domains.

RECOMMENDATION 4.

Given the underachieving results found in the current state of the art in BTP, a careful evaluation of any new biometric protection approach should be performed as a pre-requisite before any implementation in ECRIS.

Such an evaluation should be carried out on a subset of the operational fingerprint data that can be found in ECRIS (and not the ones provided by the producer of the biometric protection system).

3 Challenges of integrating an AFIS in a decentralized ECRIS architecture

A typical AFIS is composed of three main modules:

- an acquisition scanner,
- a feature extractor coupled with a matcher,
- a quality metric algorithm(s).

Depending on the architecture chosen for the AFIS and the privacy safeguards implemented, several aspects have to be taken into account for each of these three modules in order to achieve the best possible accuracy.

3.1 Acquisition scanner

Live-scanned fingerprints (most usual scanners are based on optical technology) is nowadays the most extended form of fingerprint acquisition device. Samples acquisition uses sensors that directly produce a digital image of the fingerprint. In general, optical scanners produce the best quality compared to inked fingerprints whose being acquired on an ink pad and a paper which is digitalized with a scanner.

Fingerprint scanner in ECRIS. Given the nature of ECRIS, the acquisition scanners are by definition *decentralized* as they are spread all over the EU, located in MS police precincts where the person under arrest will be taken to.

AFIS accuracy usually improves if all fingerprint samples are acquired using the same scanner model. This way, although it is not mandatory, it is advisable to have the same scanners in all acquisition sites. Knowing that this is almost unfeasible, it is desirable that they are at least as compatible as possible, for instance: same acquisition technology (e.g., optical), same resolution (e.g., 500 dpi).

It is also important to define the way in which fingerprint images are stored after they have been acquired (in order to make it as consistent as possible across acquisition sites). Typically, in order to obtain the best possible results, all 8 fingerprints and 2 thumbs are acquired and stored in a standard 10-print "container" like for instance the NIST container.

3.2 Feature Extractor and Matcher

A feature extractor receives as input the fingerprint image acquired with the scanner and extracts all the necessary features (e.g., minutiae points) to be stored in the fingerprint template.

A matcher takes as input two fingerprint templates and outputs a similarity score between the two. In the case of an AFIS this process is repeated with the n templates stored in the index/database.

The feature extractor and the matcher are usually designed and provided by the same producer which will "optimise" the matcher in the light of the feature extractor output.

Feature extractor and Matcher in ECRIS. Both the feature extractor and the matcher in ECRIS can be either: A) *centralized*, that is, one unique feature extractor and matcher for all the MS; B) *decentralized*, that is, one feature extractor and matcher for each MS.

Since it has already been established that the preferred solution will be a decentralized one (B), in the following we will present some considerations to be taken into account for this type of architecture.

Any difference between the matcher modules in two MS will potentially produce different results. Therefore, in the context of ECRIS, if exactly the same results are required in all MS, assuming a decentralized architecture, some strategy must be devised to have exactly the same matcher in all MSs and to update all the copies of the software whenever it is modified in one MS.

Also, the matcher of a given vendor is specifically designed to give the optimal accuracy with the templates produced by the feature extractor of that specific vendor. That is, just as an example, a matcher developed by 3M will in principle only work on: 1) proprietary templates produced by the 3M feature extractor; 2) standard templates generated according to the NIST or ISO standard. From those two options, the best accuracy will be reached with the proprietary templates. What is certain is that 3M matcher will not work with other proprietary templates such as Morpho, and vice versa.

Therefore, assuming that: 1) the same results must be guaranteed across all MSs and that 2) the AFIS in ECRIS should present optimal accuracy, then a strategy has to be devised in order to have the same feature extractor and matcher in all MSs and to update all the copies of the software whenever it is modified in one MS.

3.3 Quality metric algorithm(s)

A biometric quality estimator, or a biometric quality metric, is essentially an algorithm that receives as input a biometric sample (i.e., a fingerprint image) and outputs a score that can be interpreted as an estimation of how well that sample will perform in terms of recognition accuracy. In other words, it is a module that lets the operator know if the sample which has just been acquired is well suited for recognition purposes. As such, it is usually used as a first measure to improve the samples acquisition: should the fingerprint images not exceed a given quality threshold the operator is asked to reacquire the sample.

Similarly to the feature extractor and the matcher case, each AFIS vendor has his own specific quality metric that gives the best results at predicting the accuracy of their own matcher.

Quality metric algorithm in ECRIS. In order to optimize the final accuracy, in a decentralized AFIS such as the one envisaged for ECRIS, it should be recommended in principle that all users (i.e., Member States) implement the same quality metric algorithm provided by the AFIS vendor.

Although there is no specific standard regarding quality metrics, the NFIQ and NFIQ-2 developed by US NIST have become two largely deployed algorithms which in many cases are taken as the de facto standard. These two metrics have shown significant interoperability across matchers from different vendors. Accordingly, it is worthwhile to consider their inclusion in any AFIS system (in addition to the quality metric provided by the vendor) as they can serve as a normalizing quality value between the different proprietary quality metric used by each MS.

RECOMMENDATION 5.

Assuming a decentralized architecture, the designers of the AFIS should take into careful consideration:

- the characteristics of the acquisition scanners to be used (e.g., optical, 500 dpi);
- the format in which fingerprint images are stored (e.g., 10-print NIST container);
- the format of the fingerprint templates (e.g., proprietary format of the vendor providing the feature extractor *and* matcher, or ISO);

- a methodology to maintain exactly the same feature extractor and matcher in all MSs;
- the definition and deployment of common quality metric algorithm among all users.

3.4 Other architectural considerations

3.4.1 Type of fingerprint data to be stored in the index-filter

In a criminal AFIS, whenever there is a hit, this result is usually verified by a human forensic expert who bases his/her decision on the comparison of the original fingerprint images (not the templates). A similar practice is applied for EURODAC. Therefore it is assumed that the original fingerprint images are kept in the criminal record of the TCN and that this is part of the information that will be sent by ECRIS in case there is a hit in a different MS. In order to evaluate the possible impact of the different categories of biometric information to be stored in the index-filter, some of the most relevant elements to be taken into account in case fingerprint images and/or templates are stored in the index-filter are presented hereafter.

Fingerprint images stored in the index-filter:

- Fingerprint images are raw biometric data and therefore can be processed by any feature extractor and matcher.
- Any fingerprint quality metric score can be extracted from fingerprint images.
- From a privacy point of view, the leak of fingerprint raw images can potentially be more harmful than the leak of templates only.
- No research so far has been conducted on the possibility to extract features from protected fingerprint images. As such, should images be stored in the index-filter (even if they are protected), at some point they would have to be un-protected in order to carry out the feature extraction and produce the template.
- The confirmation by a dactyloscopic expert can take place immediately after a hit result, without requiring the full criminal record to be sent.

Template stored in the index-filter:

- Fingerprint templates can only be compared by the matcher developed from the same vendor that produced the template. Only standard templates (i.e., following the ISO or NIST standard) can work on virtually any matcher, however, this entails a drop in accuracy with respect to the use of the vendor proprietary templates (as pointed out in Sect. 3.2)
- Fingerprint quality metrics cannot be extracted from fingerprint templates. Therefore, all quality metrics should be estimated at the time the template is produced.
- From a privacy point of view, a leak of fingerprint templates is less harmful than a leak of the raw images. Even if, as has been pointed out in Sect. 2.1.1, it is potentially possible to reverse engineer a template and recover a fingerprint image similar to the original one (i.e., privacy challenge 1: inverse biometrics), this is by no means a straight forward process and success is not guaranteed.
- Fingerprint templates can be in principle matched in the protected domain. It should not be forgotten, however, that the matching of protected templates entails a significant loss in recognition accuracy with respect to the matching of non-protected templates (as already pointed out in Sect. 2.3)

RECOMMENDATION 6.

Storing fingerprint images in the index-filter seems to grant the highest level of interoperability. A single quality metric algorithm should be adopted with this option.

Storing fingerprint templates remains feasible and in principle providing more privacy safeguards but would require more investment from Member States which will have to use ISO-compliant templates produced from the national AFIS.

3.4.2 Unique or separate indexes for alpha-numeric and fingerprint data

Regarding the shared index-filter, another question to be addressed with the inclusion of fingerprints is the type of entries such index will contain *for each user*:

- a) Two separate pseudonymised entries, one for alpha-numeric data and one for protected fingerprint templates. This could even be interpreted as two different pseudonymised indexes: one for fingerprints and one for alpha-numeric data.
- b) One unique pseudonymised entry created through the combination of the alpha-numeric data and fingerprint data of the user.

Following the discussion for BTP algorithms presented in Sect. 2.3, no research or experimental evaluation has been carried out so far on the combination in one unique protected template of alpha-numeric and fingerprint data. Since the recognition accuracy of BTP approaches with only fingerprint data is still very low, it is expected that the combination with alpha-numeric data would make it drop even more (given that it is a more challenging scenario).

Given the difficulty of integrating in the same index-filter both alpha-numeric and fingerprint data, in the following we will assume an architecture with two separate index-filters. The next two diagrams (Figs. 1 and 2) show a possible flow chart of how the enrolment and consultation processes would be conducted at MS level:

- *Enrolment*: is the process by which a new TCN is added to the index-filter.
- *Consultation*: is the process in which the AFIS is used to search if a given TCN is already present in the index.

It should be noted that, in general, an enrolment will be preceded by a consultation as, before introducing a new individual (i.e., TCN) in the system, the MS should check if that given individual is not already in the system.

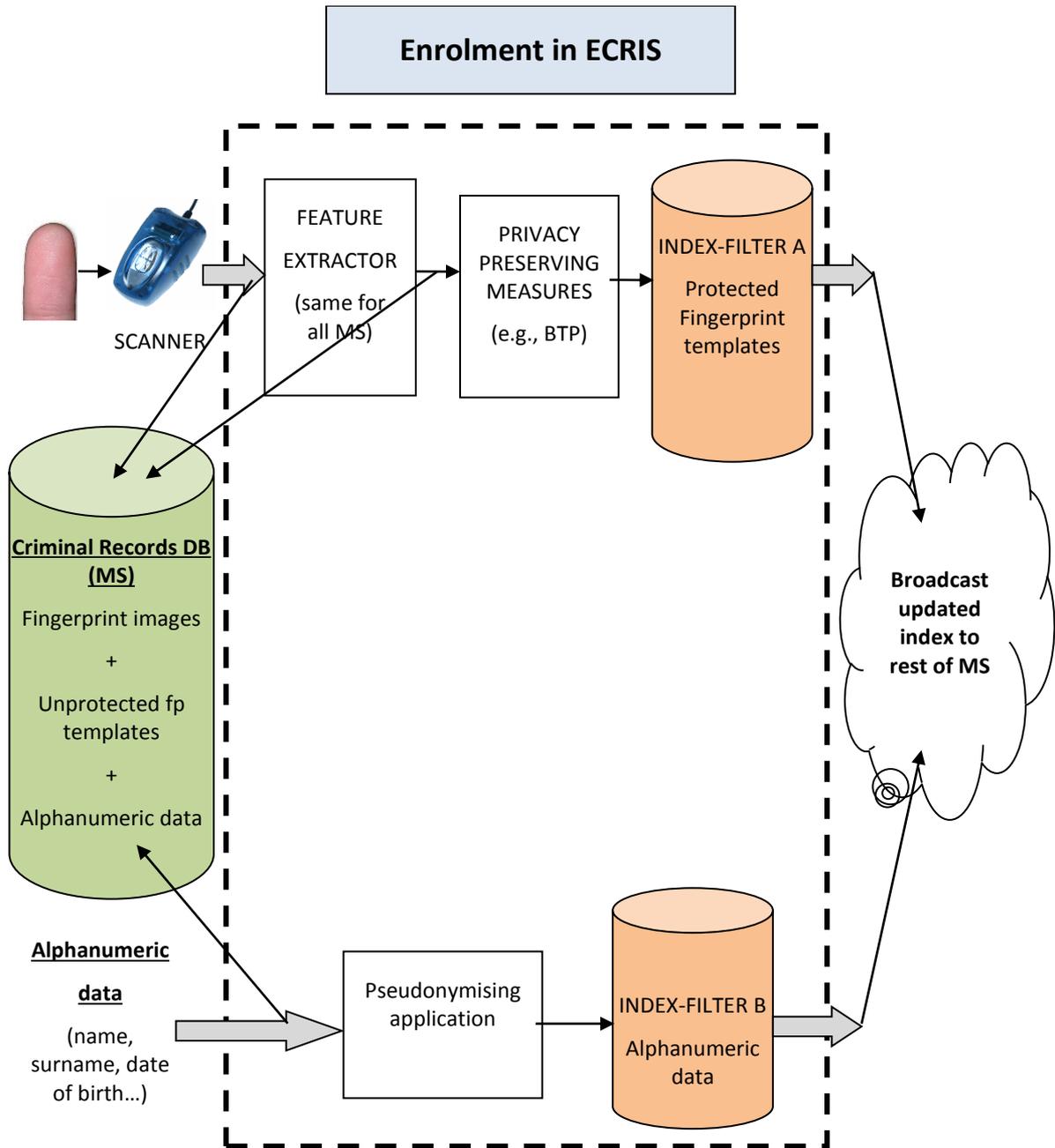


Figure 1 Diagram of the enrolment process in ECRIS assuming an architecture with two separate indexes, one for alphanumeric data and one for fingerprint data.

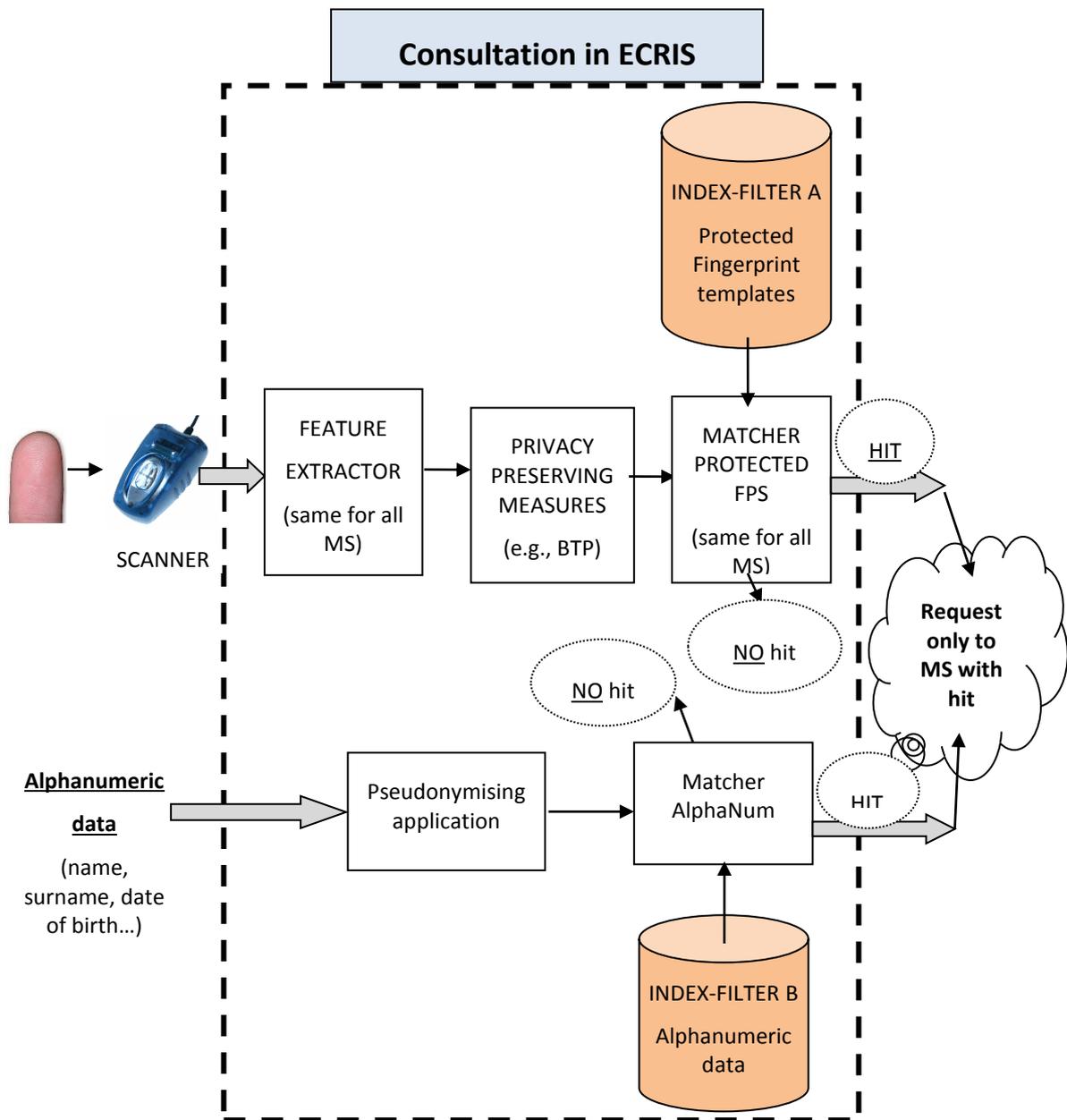


Figure 2 Diagram of the consultation process in ECRIS assuming an architecture with two separate indexes, one for alphanumeric data and one for fingerprint data.

RECOMMENDATION 7.

In case the option for data pseudonymization remains, if the expected very low performance accuracy offered is considered acceptable for ECRIS, it is recommended to develop two different index-filters (shared by all MS): 1) an index-filter for alphanumeric data; 2) a second index-filter for fingerprint data, protected for example with some of the algorithms presented in Sect. 2.3.

3.4.3 Unique or separate entries for TCN convicted in different MS.

In addition to the challenge presented in Sect. 3.4.2 (i.e., one or two index-filters for alpha-numeric and fingerprint data), a second question to be addressed is how will the index-filter(s) be managed if a MS wants to enrol a TCN that is already present in the system.

In order to address this architectural challenge a use case is proposed: let's assume that the same TCN is arrested in all 28 MSs. The possibilities to manage the index-filter will be the following ones:

- A. There is just one entry in the system for this TCN. Each time he/she is arrested the entry is updated. A strategy should be devised for the update of the entry. Who is responsible for updating the entry? Can a single entry refer to different criminal records (one in each MS)? Can France update an entry of the index-filter created by Belgium?
- B. There are 28 entries in the system for the same TCN. All 28 entries should be linked somehow. When a consultation is conducted using the AFIS, the index-filter can potentially produce up to 28 hits, one per MS. In this case, the AFIS will not perform one unique search, but 28 searches (one for each section of the index-filter corresponding to each MS).

In the case of option A, the architecture of one unique index-filter implies that:

- Any MS can modify the entries of any other MS (or can ask the other MS to do it)
- The index is not a "mirror" or a pseudonymised copy of the DB's holding the criminal records of TCN in each MS. That is, each entry in the index-filter will correspond to one or several criminal record in one or multiple MSs.

Option B implies that the index-filter can be seen as the following structure:

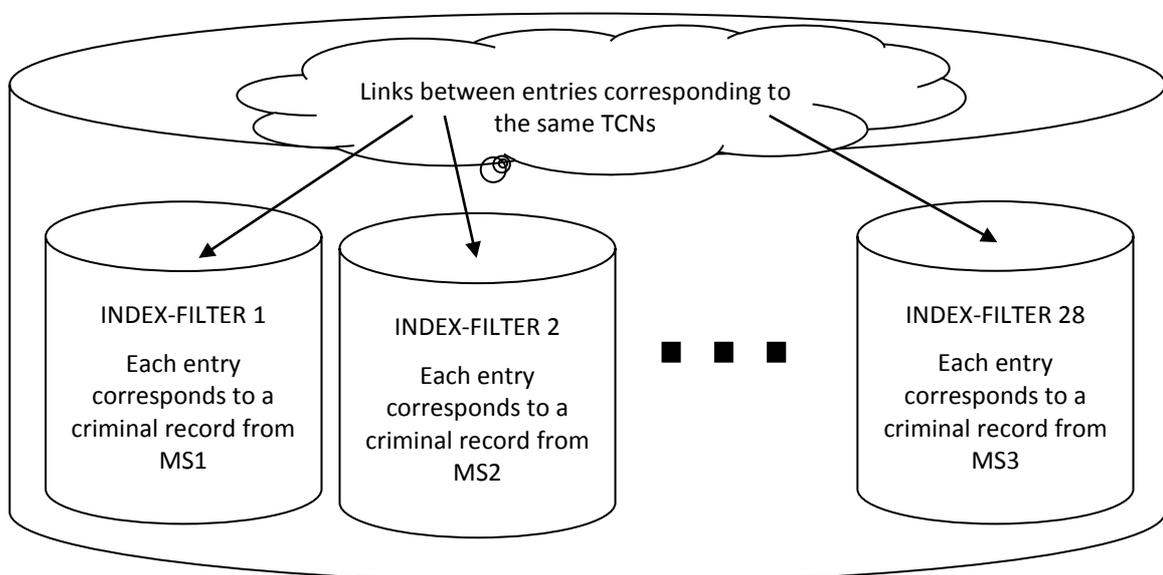


Figure 3 Diagram showing the structure of the index-filter assuming that a separate entry is kept when the same TCN is arrested in different MSs.

Such an architecture implies that:

- Each MS can only modify the entries contained in the section of the index-filter related to that MS.
- Each entry in the index-filter corresponds to a criminal record in a MS.
- The AFIS can return up to 28 hits. It will conduct a separate search for each section of the index-filter corresponding to each MS.
- There is the need to maintain a structure with the links between the entries of each of the 28 sub-indexes that correspond to the same TCNs (i.e., individuals that have been arrested in more than one MS).

4 Conclusions and Recommendations

AFIS functionality constitutes a promising and mature solution for addressing successfully the growing challenges of TCNs criminal records in ECRIS.

Biometric protection template as suggested for the pseudonymisation of the index-filter seems not to have reached the Technology Level Readiness which can be expected for ECRIS and will therefore not offer the required accuracy and processing time performance.

Several feasible options can be elaborated in order to address and preserve the founding pillars of ECRIS such as a decentralised system benefiting from a high level of security and privacy, and without compromising the performance results which can be expected from a modern AFIS.

The different conclusions and recommendations presented in the note are reproduced hereafter.

OVERALL ASSESSMENT

The current proposal for the inclusion of an AFIS within ECRIS, based on a decentralized architecture with a pseudonymized index-filter shared by all MS, presents severe flaws that will most likely lead to a failure of the fingerprint-based search engine.

The pseudonymised dimension of the index-filter has been identified as the element of the proposal that will jeopardize the performance of the envisaged system new AFIS.

RECOMMENDATION 1.

The inclusion of an AFIS within ECRIS seems to be the most suitable solution (and possibly also the only solution) to deal with the challenges that TCN currently pose to the ECRIS system.

RECOMMENDATION 2.

The most appropriate way to address potential privacy challenges in the context of ECRIS is to conduct a Data Protection Impact Assessment which will identify and quantify the risks related to the system in production and to evaluate the appropriateness of the security measures foreseen. Undermining privacy risks will have the same negative effect as overshooting them.

A good starting point is to assess the security measures and data protection requirements already applied to similar national criminal systems or at least such as EURODAC.

RECOMMENDATION 3.

We recommend to carefully assess to which extend irreversibility, unlinkability, accuracy and speed are required for the implementation of an AFIS in ECRIS:

- Should irreversibility be granted?
- Should unlinkability be granted?
- What is the expected minimum accuracy of the AFIS (at least equivalent to those national ones)?
- What is the expected speed of the AFIS (at least equivalent to those national ones)?

RECOMMENDATION 4.

Given the underachieving results found in the current state of the art in BTP, a careful evaluation of any new biometric protection approach should be performed as a prerequisite before any implementation in ECRIS.

Such an evaluation should be carried out on a subset of the operational fingerprint data that can be found in ECRIS (and not the ones provided by the producer of the biometric protection system).

RECOMMENDATION 5.

Assuming a decentralized architecture, the designers of the AFIS should take into careful consideration:

- the characteristics of the acquisition scanners to be used (e.g., optical, 500 dpi);
- the format in which fingerprint images are stored (e.g., 10-print NIST container);
- the format of the fingerprint templates (e.g., proprietary format of the vendor providing the feature extractor *and* matcher, or ISO);
- a methodology to maintain exactly the same feature extractor and matcher in all MSs;
- the definition and deployment of common quality metric algorithm among all users.

RECOMMENDATION 6.

Storing fingerprint images in the index-filter seems to grant the highest level of interoperability. A single quality metric algorithm should be adopted with this option.

Storing fingerprint templates remains feasible and in principle providing more privacy safeguards but would require more investment from Member States which will have to use ISO-compliant templates produced from the national AFIS.

RECOMMENDATION 7.

In case the option for data pseudonymization remains, if the expected very low performance accuracy offered is considered acceptable for ECRIS, it is recommended to develop two different index-filters (shared by all MS): 1) an index-filter for alpha-numeric data; 2) a second index-filter for fingerprint data, protected for example with some of the algorithms presented in Sect. 2.3.

References

- [Barni et al., 2010] M. Barni, T. Bianchi, D. Catalano, M. di Raimondo, R. D. Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, A. Piva, and F. Scotti. “A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates”. *In Proc. Int. Conf. on Biometrics: Theory Applications and Systems, BTAS*, pages 1-7, 2010.
- [Boult, 2006] T. Boult. “Robust distance measures for face-recognition supporting revocable biometric tokens”. *In Proc. Int. Conf. on Automatic Face and Gesture Recognition, FGR*, pages 560-566, 2006.
- [Bringer et al., 2013] J. Bringer, H. Chabanne, and A. Patey. “Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends”. *IEEE Signal Processing Magazine*, 30(1):42-52, 2013.
- [Campisi, 2013] P. Campisi, editor. *Security and Privacy in Biometrics*. Springer, 2013.
- [ISO/IEC 2011] ISO/IEC JTC1 SC27 IT Security Techniques. ISO/IEC 24745:2011. Information Technology - Security Techniques - Biometric Information Protection. International Organization for Standardization, 2011.
- [Nandakumar et al. 2007] K. Nandakumar, A. K. Jain, and S. Pankanti. “Fingerprint-based fuzzy vault: Implementation and performance”. *IEEE Trans. on Information Forensics and Security*, 2(4):744-757, 2007.
- [Nandakumar 2010] K. Nandakumar. “A fingerprint cryptosystem based on minutiae phase spectrum”. *In Proc. Int. Workshop on Information Forensics and Security, WIFS*, pages 1-6, 2010.
- [Nandakumar and Jain 2015] K. Nandakumar and A. K. Jain. “Biometric template protection: Bridging the performance gap between theory and practice”. *IEEE Signal Processing Magazine*, 32(5):88-100, 2015.
- [Pillai et al., 2011] J. K. Pillai, V. M. Patel, R. Chellappa, and N. Ratha. “Secure and robust iris recognition using random projections and sparse representations”. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 30(9):1877-1893, 2011.
- [Ratha et al., 2001] N. K. Ratha, J. H. Connell, and R. M. Bolle. “Enhancing security and privacy in biometrics-based authentication systems”. *IBM Systems Journal*, 40:614-634, 2001.
- [Ratha et al. 2007] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle. “Generating cancelable fingerprint templates”. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 29(4):561-572, 2007.
- [Rathgeb and Uhl, 2011] C. Rathgeb and A. Uhl. “A survey on biometric cryptosystems and cancelable biometrics”. *EURASIP Journal on Information Security*, 2011(3), 2011.
- [Rathgeb et al., 2013a] C. Rathgeb, F. Breitingner, and C. Busch. “Alignment-free cancelable iris biometric templates based on adaptive bloom filters”. *In Proc. IAPR Int. Conf. on Biometrics ICB*, pages 1-8, 2013a.
- [Rathgeb et al., 2013b] C. Rathgeb, F. Breitingner, C. Busch, and H. Baier. “On the application of bloom filters to iris biometrics”. *IET Biometrics*, 2013b.
- [Teoh et al. 2004] A. B. J. Teoh, D. C. L. Ngo, and A. Goh. “Personalised cryptographic key generation based on FaceHashing”. *Computers And Security*, (23):606-614, 2004.

[Teoh et al., 2006] A. B. Teoh, A. Goh, and D. C. Ngo. “Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs”. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 28(12): 1892-1901, 2006.

[Vielhauer et al. 2002] C. Vielhauer, R. Steinmetz, and A. Mayerhoefer. “Biometric hash based on statistical features of online signatures”. *In Proc. Int. Conf. on Pattern Recognition, ICPR*, pages 123-126, 2002.

[Ye et al., 2009] S. Ye, Y. L. ad J. Zhao, and S. S. Cheung. “Anonymous biometric access control”. *EURASIP Journal on Information Security*, 1-17, 2009.

Annex A – Biometric nomenclature

Some biometric related nomenclature that is used throughout the present document is introduced here:

- *Biometric characteristic*: biological or behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition (e.g., the fingerprints)
- *Biometric sample*: is an analog or digital representation of biometric characteristics prior to the biometric feature extraction (e.g., in the case of fingerprints the biometric sample would typically be a fingerprint image).
- *Biometric template*: is a set of biometric features that can be directly matched to a different set of features (e.g., in the case of fingerprints the biometric template would typically be a file containing the position and angle of the fingerprint minutiae points, which in turn would be the set of biometric features).
- *Biometric matching*: estimation, calculation or measurement of similarity or dissimilarity between two biometric templates.
- *Unprotected biometric domain/system*: biometric system in which the privacy of the user is *not* preserved.
Protected biometric domain/system: biometric system in which the privacy of the user is enhanced.

Annex B – Examples of large European AFIS

Some examples of large European AFIS systems are:

	PRUM	VIS	SIS-II	EURODAC
Purpose	Criminal AFIS	Visa applicant (civil)	Border (civil) + criminal	Asylum seeker (civil)
Architecture	Peer-to-peer	Centralized	Centralized + National Copies	Centralized
DB Encrypted	YES (depending of the MS selected solution)	YES	YES	YES
Matching encrypted	NO	NO	NO	NO

***Europe Direct is a service to help you find answers
to your questions about the European Union.***

Freephone number (*):

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

More information on the European Union is available on the internet (<http://europa.eu>).

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
via EU Bookshop (<http://bookshop.europa.eu>);
- more than one copy or posters/maps:
from the European Union's representations (http://ec.europa.eu/represent_en.htm);
from the delegations in non-EU countries (http://eeas.europa.eu/delegations/index_en.htm);
by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm) or
calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (<http://bookshop.europa.eu>).

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:10.2788/26312

ISBN 978-92-79-61299-2