



Shared Biometric Matching Service (sBMS)

Feasibility Study - final report

This document is public. Reproduction is authorised, except for commercial purposes, provided that the source is acknowledged.

eulisa.europa.eu

ISBN 978-92-95208-73-5

doi:10.2857/84504

Catalogue number: EL-04-18-248-EN-N

© European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), 2018

Table of Contents

1.	Introduction	5
1.1	Background	5
1.2	Executive Summary	6
1.3	Key Business Requirements	8
1.4	Scope and Objectives	9
1.5	Methodology	10
2.	Target Architecture	11
2.1	Description	11
2.2	Description and Analysis	11
2.3	Comparison Framework	17
2.3.1	IT Security and Compliance (integrity and confidentiality)	17
2.3.2	Legal impact	20
2.3.3	Interoperability, Integration and Interconnectivity	21
2.3.4	Scalability, Capacity and Performance	24
2.3.5	Business Continuity	26
2.3.6	Flexibility	27
2.3.7	Others (Complexity of Implementation, Time to Market, Operations and Maintenance and Exit Scenarios – reversibility)	30
2.3.8	Financial Impact	33
2.3.9	Data Separation-Related Risks Overview	35
2.3.10	Summary of Comparison and Ranking	37
3.	Migration Options	38
3.1	Overview	38
3.2	Analysis and Impact Assessment	38
3.2.1	Impact Assessment Framework and Methodology	40
3.2.2	Legal Impact	41
3.2.3	Business Impact	42
3.2.4	Financial Impact	43
3.2.5	Technical Impact	44
3.2.6	Operational Impact	44
3.2.7	Impact Assessment Results	45
3.2.8	General Remarks Towards the Migration Options	45
4.	Flagging Functionality	46
4.1	Options Overview	46
4.2	Description	49
4.3	Analysis	61
4.3.1	Implementation Complexity	61
4.3.2	Cost/Change Capacity	62
4.3.3	Dependencies	62
4.3.4	Legal	63
4.3.5	IT Security	63
4.3.6	Summary of Comparison Results	64
4.3.7	Further considerations for Fittest Flagging Options	64
4.3.7.1.	High Level Network Overview	64
4.3.7.2.	Flagging Workflow, including NIST translation considerations	65

4.3.7.3.	Silent Notification and SIRENE Messages Workflow	66
4.3.7.4.	Proposed Flagging Message Design	67
5.	Conclusions and Recommendations	68

1. Introduction

1.1 Background

On 6th of April 2016, with the Communication "Stronger and Smarter Information Systems for Borders and Security", the European Commission (COM) introduced the concept of interoperability of systems in the Justice and Home Affairs domain and established it as a political priority. One of the building blocks of the foreseen interoperability architecture is a shared Biometric Matching Service (sBMS) providing horizontal standardized biometric capabilities to various large-scale information systems. To develop further the concept introduced in the Communication, the Commission established the High Level Expert Group on Information Systems and Interoperability (HLEG) to define a roadmap towards practical implementation of interoperability in the JHA domain. The HLEG, in its final report of May 2017, requested eu-LISA to 'analyse the technical and operational aspects of the possible implementation of a shared biometric matching service'. This report, delivered by eu-LISA, reflects some of the analysis undertaken on foot of this request.

At this point of time, eu-LISA is managing two different systems for biometrics matching (i.e. an Automated Fingerprint Identification System, AFIS), one for Eurodac and one for the Visa Information System (VIS). Each of them contains different types of fingerprints (i.e. rolled versus 'flat' fingerprints), is managed with the support of different vendors and is built utilising different technologies. Thus they are managed entirely independently.

In the near future, a new AFIS will be implemented to support the Schengen Information System (SIS II) (it is supposed to be operational by mid-2018). It will individually serve the SIS II system alone. In addition, the Entry-Exit System, to be developed and managed by eu-LISA according to the recently approved legislation (Regulation 2017/2226) will also rely on its own biometric matching engine. This engine will be capable of matching facial images as well as fingerprints (and may therefore be described more generally as an Automated Biometric Matching Service, ABIS). The co-legislators are also evaluating the possibility of including central biometric matching capabilities in the ECRIS-TCN central system currently being examined.

The sBMS has been conceived based on the key assumption that rather than having four or more individual biometric systems, each serving one IT system, eu-LISA and its stakeholders could benefit from implementing a unique shared biometric system that could be shared by all systems. Reduced IT complexity and costs, along with technical, financial, operational and managerial synergies have all been noted amongst the positive outcomes foreseen.

In this respect, eu-LISA had to identify and analyse the feasibility of different architectural options for the implementation of the sBMS, capable of supporting the various biometric operations of all current and future systems managed by the Agency.

To achieve this objective eu-LISA entrusted to an external independent contractor the execution of a study that had to take into account all biometrics functional and non-functional requirements of the IT systems, the state of maturity of biometric technology available on the market and eu-LISA's operational and strategic objectives in this regard. The study also included an assessment of the 'flagging' functionality highlighted in the HLEG's final report, with the possibility of the sBMS raising hit/no-hit "flags" from the various connected applications being specifically examined. This report provides an overview of the main outcomes of this study.

1.2 Executive Summary

This report reflects the main outcomes of the eu-LISA study on the feasibility of a shared biometric matching service.

The study sought to examine possible future architectures for such a service. The architectures were elaborated following an in-depth assessment of the current state of eu-LISA's biometric services and the availability of modern solutions for such purposes on the market. The different architectural options were compared based on their capabilities to fulfil functional and non-functional requirements of current and future applications and the extent to which they fulfil the main objectives of the sBMS. Possible approaches to migrating to the different setups were considered along with the associated impacts. Finally, the extent to 'flagging' could be possible within the elaborated setups was studied.

Initial work focussed on elaboration of a clear picture of the existing systems, their requirements and high-level architectures. This provided a solid ground for defining possible scenarios for the sBMS. It was noted that there are some reusability options within the current Eurodac and VIS/BMS solutions, depending on the common ABIS (Automated Biometric Information System) scenario. However, a more detailed analysis of the financial feasibility of reusing the components would be needed as soon as the exact architecture and configuration is defined and agreed amongst all relevant stakeholders.

When considering the current state of maturity of biometric technology, it was found that the biometrics market is progressing at a high speed, introducing new opportunities for border control and law enforcement. Leading vendors are improving their current offerings to cover new functionalities and biometric modalities. There are also new emerging vendors who are bringing innovative biometrics solutions to the market.

Throughout the study, technical possibilities were assessed based on the offerings of vendors whose capabilities were considered as representative of the market as a whole. As rationale for selecting the vendors, the study took into account publicly available information and vendors' proven track record regarding capabilities for delivering with the required accuracy in the context of large-scale biometric projects in the public service, including outside their home countries. Exclusion criteria were defined while capabilities to support multi-modal biometrics, namely facial images, fingerprints (latent, rolled, flat, slap), iris and palm, to provide high matching accuracy, reliable recognition and to guard against spoofing attacks were considered. Additionally, the vendors' support for both verification (1:1 verification, border control) and identification (1:few, 1:n, law enforcement, asylum) was taken into account.

Taking into account all information obtained from eu-LISA and the identified large-scale ABIS providers, 6 potential architectural options were identified and further assessed across 8 relevant criteria presented below within the report, namely: IT security and compliance; impact on legal basis; integration and interconnectivity; scalability, capacity and performance; business continuity; flexibility; others like complexity of implementation, time to market, operations and maintenance, reversibility and financial impact.

The options, described fully later, were:

Option #1: Fully separated architecture (continuation of AS-IS situation)

Option #2: Multiple ABIS, templates in multiple data store

Option #3: Common ABIS, logically separated template data stores

Option #4: Multiple ABIS, logically separated template data stores

Option #5: Common ABIS, shared template database

Option #6: "common Shared Biometric Service Platform (cSBSP) - Multiple matchers, logical separation of templates

All consulted vendors could support all options outlined. Although no final decision is made on the appropriate option to pursue, taking into account a full cost-benefit analysis, the balanced view presented in which no particular criteria are more heavily weighted than others leads to the conclusion that option #6 could be considered as a favoured option.

Implementation of any of the analysed architectural options (with the exception of the 1st which is an optimised version of the current setup) would require a migration from the current setup. Therefore, the study also analysed several identified migration scenarios. Pros and cons of each approach are outlined without any particular conclusion being drawn regarding an optimal approach.

Finally, the feasible approaches to incorporating flagging functionality into the outlined architectures were examined. This built upon the previously analysed topics, with the analysis undertaken also considering possible function of the sBMS alongside other concepts proposed by the HLEG, particularly the European Search Portal (ESP) and Common Identity Repository (CIR). It was established that flagging functionality could be included no matter which sBMS architectural option would be chosen as a future model. Possible synergies with the ESP and CIR could also be foreseen. Final selection of the appropriate design option would require consideration of the main outcomes desired by stakeholders and specific study of the ESP and CIR concepts.

1.3 Key Business Requirements

As a long-term objective, eu-LISA intends to work towards the implementation of a sBMS that could be shared by existing and any future systems managed by eu-LISA. This means that the shared biometric system must meet all of the functional and non-functional requirements of the existing systems (Eurodac, VIS/BMS) and planned systems (EES, SIS II AFIS) and be highly adaptable to any not yet concretely foreseen additional systems. In addition, the common ABIS should be accessible for use by external partners (e.g. Europol) as a service (serve as a shared service platform), potentially within a hub environment.

The key requirements include:

Functional requirements

- Verification (1:1) and identification (1:n) with fingerprints
- Verification (1:1) and identification (1:n) with facial image
- Latent search (1:n)
- Multimodal search (FP & FI) and fusion (i.e. the use of more than one biometric modality at once to make a single decision regarding a person's identity)
- The possible extension of capabilities to palm print matching, iris recognition and matching of other biometric modalities
- Availability of all necessary associated operations including CUD (Create, Update, Delete), linking and quality control operations on fingerprints, facial images and other relevant data types (e.g. other biometric modalities, latent mark-up etc.).

Technical requirements

- High availability, performance, capacity, scalability, accuracy and continuity of the biometric services

Other requirements

- Compliance to the security and data privacy requirements set by EU regulations and in line with agreed upon principles and guidance provided by relevant authorities, such as the European Data Protection Supervisor (EDPS) and the EU agency for Fundamental Rights (FRA)
- Compliance to the data retention requirements set by EU regulations.
- Support for business rule changes and/or vendor changes

1.4 Scope and Objectives

The scope of the study was carefully delineated to address current gaps in knowledge with regard to the feasibility of the sBMS concept and to assess impacts of the possible future implementation of the sBMS on relevant stakeholders. The possible architectures of a future sBMS that would be capable of fulfilling all requirements noted in section 1.3 were analysed in depth, building upon analyses of current technological possibilities and best practices. Options for migration to these architectures from the current 'as-is' setups were also assessed, taking into account the as-is situation and reflecting upon the impacts on various parties. Finally, the possible offering of new functions to end users within the architectures outlined was considered, with focus on the proposed 'flagging' functionality. The chapters that follow deal with each aspect in turn.

The study does not examine specific questions related to biometric performance or the future setup of any sBMS (e.g. threshold setting, error rates, fusion performance etc.) as such analyses typically require testing against large-scale datasets. Indicative data on general performance capabilities of modern biometric algorithms is also available from other parties such as the US National Institute of Standards and Technology (NIST).

Beginning by drawing a clear picture of the existing situation (as-is) and including an exhaustive list of services that could be re-used (with an exhaustive list of weaknesses and strong points of the current biometrics architecture), the study then goes on to identify and analyse a number of future scenarios in line with best practices on biometrics technologies (gap analysis). It includes an assessment of the alternative solutions to the current BMS technology in order to show the different possibilities which eu-LISA might consider, while also covering the financial, technical, operational and maintenance impact of each option. Furthermore, the effort (time, costs and organisation) required to achieve migration from the existing infrastructure to the target infrastructure (to-be), for each scenario, was also assessed with a view towards outlining a more solid biometric technology roadmap for the next 5-6 years.

The following specific assessments were included within the study:

Assessments	Key Outcomes
Current State Assessment (as-is)	Scope and guiding principles for strategy defined Final set of deliverables agreed Draft template of study outcome
Target Architecture Definition and Identification	Target architecture proposal defined Reference Architecture defined, based on an industry-leading infrastructure stack
Achieving the targeted migration and work for the proposed solutions	Main solutions identified and defined Consolidated roadmap defined Time, costs and organizational indications provided
Target Architecture Definition, Identification and migration options for	'Flagging' target architecture options defined 'Flagging' Reference Architecture defined and options for implementation/migration

solutions proposed with 'flagging functionality'	Consolidated 'flagging' roadmap defined Time, costs and organizational indications provided
--	--

1.5 Methodology

The data gathering approach was based on obtaining a quick and aggregated overview of eu-LISA's key systems and their key functional and non-functional requirements. The collection approach was based on obtaining the best overview possible considering the constraints of data availability. The current state data was gathered from existing documentation, supplemented with information derived from a series of interviews with key stakeholders. The market overview was based on data obtained from Research and Consulting materials, major biometric vendors and public sources.

A detailed description of the process followed in delivery of the study is depicted in the chart below.

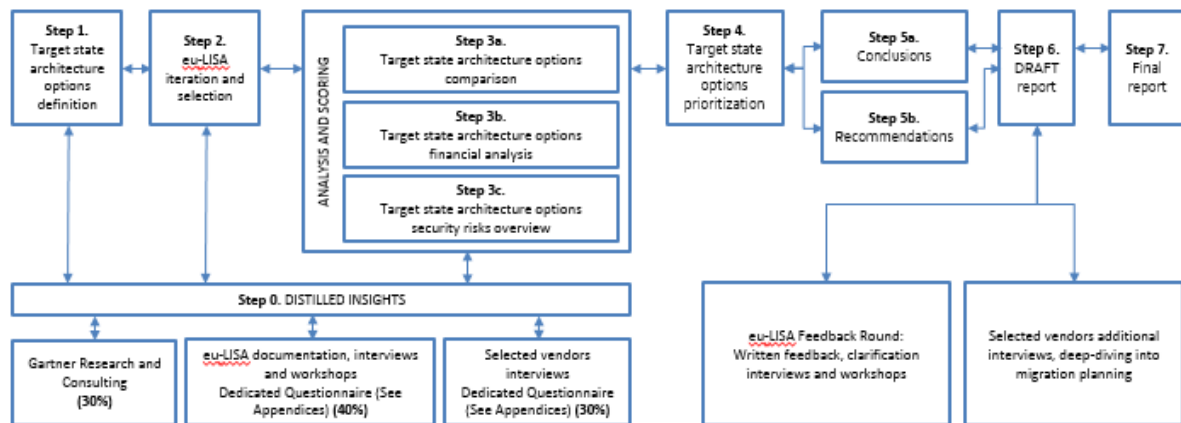


Figure 1. General approach to the study

2. Target Architecture

2.1 Description

The proposed target architecture options were selected based on a high-level assessment of each option's ability to meet the security requirements and to provide cost and efficiency improvements (exclusion criteria), with no negative impact on business services offered to Member States. The comparison of the proposed target architecture options is based on insights from research, eu-LISA additional interviews and workshops, and from conducted interviews with selected biometrics vendors.

2.2 Description and Analysis

The following 6 possible target state architecture options were identified for the current and future ABIS platforms managed by eu-LISA. Note that in all diagrams that follow, shared elements are shown in colour; databases storing biometric templates are shown in green, matching engine layers in blue and application logic in orange/yellow:

Option #1: Fully separated architecture (continuation of AS-IS situation).

EES, Eurodac, SIS II ABIS, VIS and potential other future systems are fully "air-gapped". As a result, no direct communication is possible between the different systems, except the planned interoperability between VIS and EES. This is the continuation of the current state. Member States may have a single search interface to query across several applications/ABIS simultaneously to produce combined results on one single screen - the proposed European Search Portal (ESP) at central level could also facilitate such queries. Each individual system's (EES, Eurodac, SIS II ABIS, VIS, etc.) HW usage and operations can be optimized by virtualizing the server architecture. To enhance the availability and performance, the target technical architecture of each individual system can be based on an active-active setup of the CU (Central Unit). The fully separated target architecture option needs to undergo similar changes to the current architecture to support a potential active-active setup.

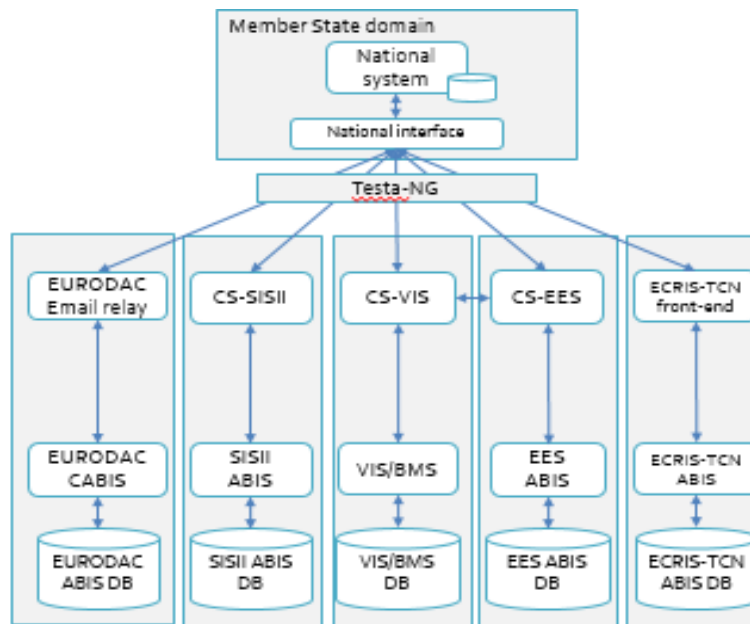


Figure 2. Architectural option 1

Option #2: Multiple ABIS, templates in multiple data stores.

Although the configuration differs, the basic building blocks are the same as for the first option. This extra configuration can be applied to a standard ABIS template instance to make it specific to the system (e.g. required accuracy, authorization profile...). Virtualization could be used in this option to improve cost and operational efficiency. Because, in such instances, the ABIS software runs in completely separated Virtual Machines (VMs), there is no risk that in one ABIS instance fingerprint data exists in-memory for more than one system, or that with a single configuration error unauthorized access is possible. Since the systems are no longer “air gapped”, a Security Information and Event Management (SIEM) solution can correlate events from the different platforms. This ensures that any breach can be immediately detected and mitigated. When multi-modal biometrics is required, use of a special BMS image to limit required expensive licenses would be feasible. The fully standardized, stateless virtual ABIS images could run on the same physical hypervisors. Images could be configured and deployed automatically by scripts. Each individual system (EES, Eurodac, SIS II, VIS, etc.) would use a common Enterprise Service Bus (ESB) running on a hypervisor. The common ESB would only need to be created once. The setup of this ESB, nevertheless, would need to be very highly available in order to avoid single points of failure. In order to enhance the degree of IT security, all ABIS systems are in a different logical network segment, separated with firewalls that stop all non-management traffic.

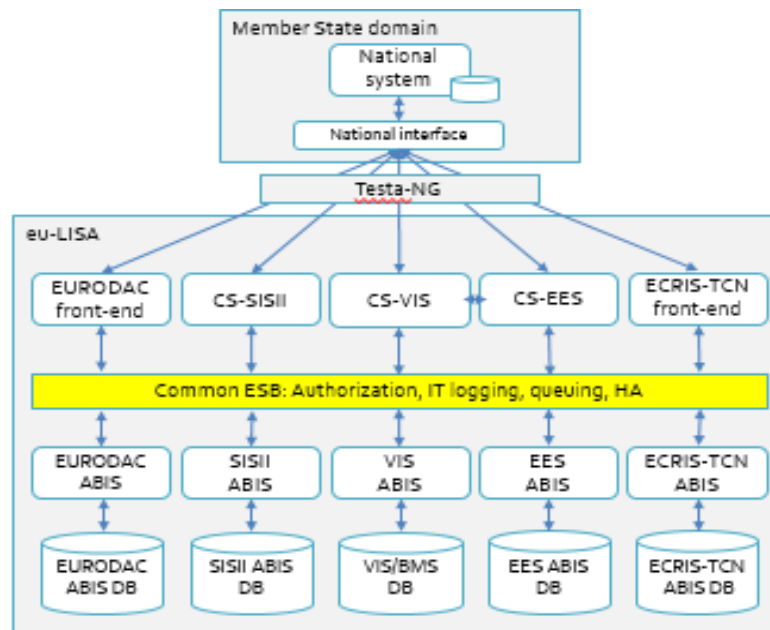


Figure 3. Architectural option 2

Option #3: Common ABIS, logically separated template data stores

According to this option, EES, Eurodac, SIS II, VIS and potential other future systems are separated virtually but may access the same ABIS. The shared ABIS has a common repository of biometrics templates, however with data separation maintained and with possible use of separate matchers. In this approach, the maximum level of efficiency can be obtained because only one ABIS instance has to be maintained. On the other hand, there is restricted possibility to use business-specific biometric configurations per Central System. The ABIS system is a “black box” security wise. Analysis showed that ABIS providers have limited application security built in. As a result, some risk was perceived that a single IT security issue/configuration error could be sufficient to “break” from e.g. SIS II to Eurodac data, because it exists on the same virtual server.

Monitoring in this case is more difficult because it is not possible to rely on Virtual Machines or network logging to detect any breach. Each individual system (EES, Eurodac, SIS II, VIS, etc.) would use a common ESB running on a hypervisor. The ESB orchestrates the requests to the common ABIS on the same hypervisor. The common ESB only needs to be created once. The setup of this ESB needs to be very highly available in order to avoid single points of failure. The same applies to the ABIS. Thus, an active-active set-up would be recommended as a prerequisite if development was to be pursued according to this option.

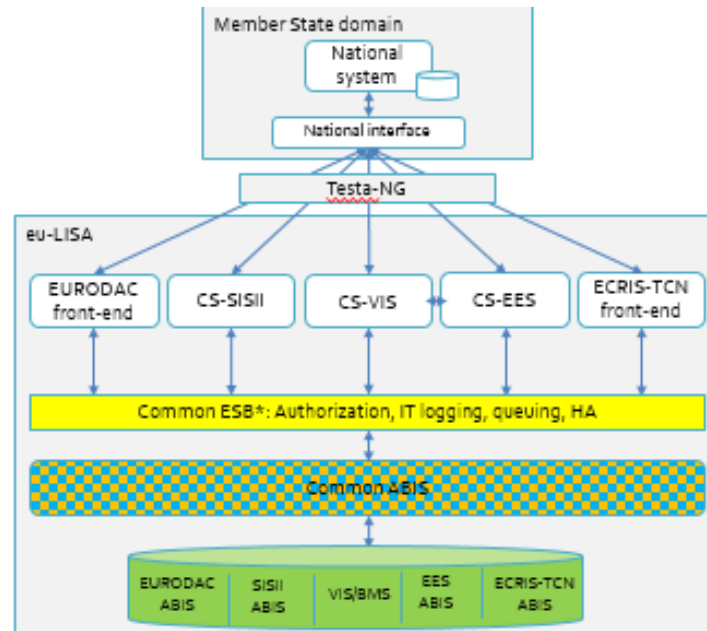


Figure 4. Architectural option 3

Option #4: Multiple ABIS, logically separated template data stores

For this option, in order to enhance the degree of IT security, all ABIS systems are in different logical network segments. The database is shared by all ABIS. Fully standardized, stateless virtual ABIS images run on the same physical hypervisors. Images could be configured and deployed automatically by scripts. Each individual system (EES, Eurodac, SIS II, VIS, etc.) would use a common ESB running on a hypervisor. The common ESB only would need to be created just once. The setup of this ESB needs to be very highly available in order to avoid single points of failure.

The ABIS in this case can be considered as having the same pros and cons as for option 2. Compared to option 3, logical separation of data is guaranteed. Yet since the systems are no longer “air gapped”, a Security Information and Event Management (SIEM) solution can correlate events from the different platforms. This ensures that any breach can be immediately detected and mitigated. Because the database is combined, there is some risk of configuration error.

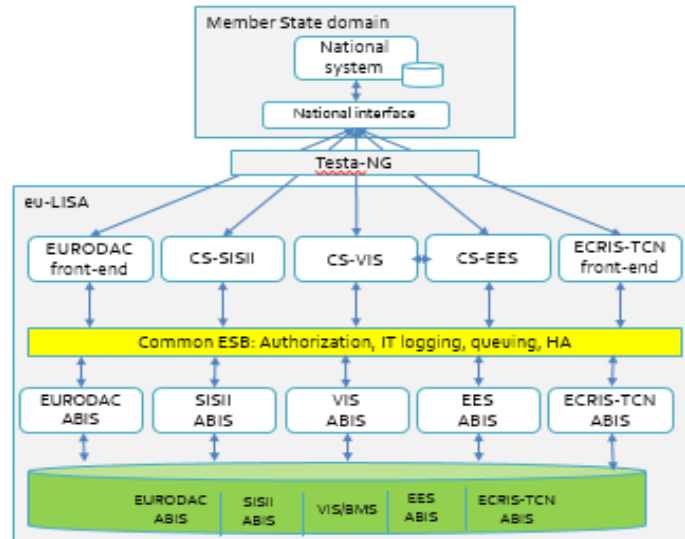


Figure 5. Architectural option 4

Option #5: Common ABIS, shared template database

For option 5, the biometric template data is shared in a single database. Additionally, a single ABIS layer is common to all systems. In this approach, the maximum level of operational efficiency can be obtained because only one ABIS instance has to be maintained. But the ABIS system is a “black box” security wise, as for option 3. Furthermore, in case of a disaster, the impact would be horizontal across all systems. There is limited possibility to use business-specific biometric configurations per CS.

Considering the option in detail, it would be suggested that each individual system (EES, Eurodac, SIS II, VIS, etc.) use a common ESB running on a hypervisor. The ESB would orchestrate the requests to the common ABIS on the same hypervisor. The common ESB would only need to be created once.

The setup of this ESB needs to be very highly available in order to avoid single points of failure. The same applies to the ABIS. Thus, active-active set-up would be recommended for this option.

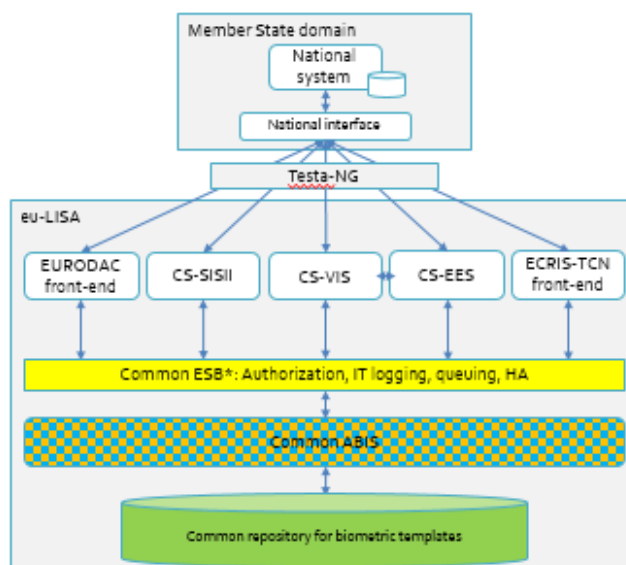


Figure 6. Architectural option 5

Option #6: Multiple matchers, consequent logical separation of templates

For this final option, each individual system (EES, Eurodac, SIS II, VIS, etc.) communicates through a common ABIS-Gateway and a consecutive ABIS Orchestration Layer (AOL) with different, possibly specific, matcher(s), all running on platform hypervisors. The different matchers may be configured to be system specific and could use dedicated resources (e.g. required accuracy, modality, performance...). The images could be configured and deployed automatically by scripts.

Logical separation of data is managed and ensured via the ABIS-orchestration. Since the systems are no longer “air gapped”, a Security Information and Event Management (SIEM) solution could correlate events from the different platforms. This would help to ensure that any potential breach would be detected and steps taken to mitigate such risks. Potential misconfiguration of the common repository-database is liable to have inter-service impacts but is at the same time mitigated through the logical separation of individual databases managed by one common database management system.

The setups of the ABIS-Gateway and AOL would need to be of a very high availability / redundant in order to avoid single points of failure. This makes Active-Active Design practically a prerequisite.

This architecture has been named ‘common Shared Biometric Services Platform’ (cSBSP). The cSBSP architecture was elaborated within the study aiming towards offering all identified advantages of the 5 previous options considered and overcoming the identified disadvantages to the extent technically feasible. It ensures that each existing system (e.g. Eurodac, SIS II, VIS) can be individually regulated, operated and monitored (data collection, transmission, data access, retention etc.). By deliberately detaching an ABIS Orchestration Layer (AOL) from the underlying biometric matchers, a more modular architecture is achieved. By design (and in particular, because of the fact that none of the matching vendors should be placed in control of building the AOL), the Agency would assume the fullest control possible over data use and handling inside the platform.

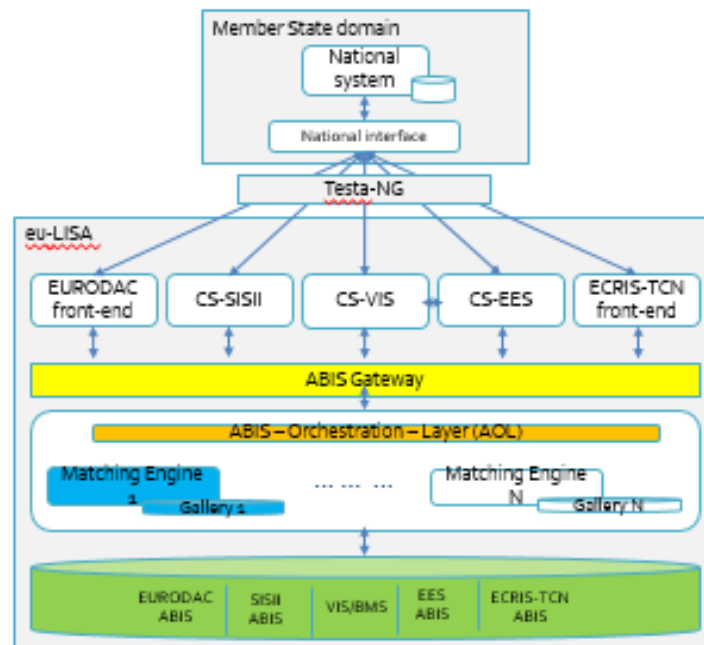


Figure 7. Architectural option 6

2.3 Comparison Framework

The proposed architectural options were compared against each other, based on their high-level application and technical architectures, in line with a set of 8 criteria. The criteria were chosen following a consultation of experts regarding the criteria typically influencing decision making related to system architectures. The criteria determined as relevant in the context of eu-LISA were agreed, grouping them in some instances where they were considered sufficiently similar.

The criteria are those typically used when evaluating the qualities of architectural options – for example, according to the Architecture Tradeoff Analysis Method (ATAM) developed by the Software Engineering Institute (see <https://www.sei.cmu.edu/architecture/tools/evaluate/atam.cfm>). They have not been specifically prioritised within this study, however, as would often be the next step of an ATAM process. Proceeding according to a balanced view of the different criteria was a preferred approach compared to policy-based prioritisation of some.

#	Criteria
1	IT security and compliance (integrity and confidentiality)
2	Other impact on legal basis
3	Integration and interconnectivity
4	Scalability, capacity and performance
5	Business Continuity
6	Flexibility
7	Others (Complexity of implementation, Time to market, Operations and maintenance, and Exit scenario's (reversibility))
8	Financial Impact

The 1-5 scoring scale is easy to understand, yet has proven its efficiency across multiple projects:

- - Very low (1), - Low (2), ± Neutral (3), + Good (4), and ++ Very good (5).

2.3.1 IT Security and Compliance (integrity and confidentiality)

In this section, IT security characteristics, including strengths/ cautions, with a focus on logging and monitoring, identity and access management (IAM), and data separation, are considered.

Target architectural options	Score	Justification
Architectural option #1: Fully separated architecture (continuation of AS-IS situation)	++	Safest option, focused on IT security, achieving maximum (data) separation, fully "air gapped". Identity and Access Management (IAM) is partly done at MS level; it is up to national system (NS) to authorize access to systems.

Architectural option #2: Multiple ABIS, templates in multiple data stores	+	The ABIS systems are not “air gapped” but running on separate virtual machines (VMs) on the same physical hypervisors, in different logical network segments. These are separated using firewalls to stop all non-management traffic. There is no risk that in one ABIS instance fingerprint data exists in-memory for more than one system because each sits in different VMs – a relevant data protection safeguard. An “air gapped” architecture is not specifically required by applicable regulations, according to the interpretation of the legal framework in force. Consultations with data protection experts suggested that logical data separation, if appropriately implemented, can be considered sufficient. A SIEM solution (log management, events correlation, alerts, dashboards, compliance, retention, forensic analysis) is used to ensure secure logical separation and immediate detection even in case of malicious penetration (beyond virtual machine and logical firewalls).
Architectural option #3: Common ABIS, logically separated template data stores	±	eu-LISA would need to trust the IT security of the ABIS system’s “black box”. A separate impact assessment would be needed. Because all data is in the same database the risk increases that due to a human configuration error, data of Central System (CS) 1 could become visible to Central System 2, or that record updates/deletes meant for Central System 1 might also be executed for system 2. Since all data resides on the same virtual network, one IT security or configuration issue could be sufficient to breach from e.g. SIS II to Eurodac data. Monitoring for these kind of breaches is far more difficult compared to the other scenarios because it is not possible to rely on VM or network logging to detect breaches. For some vendors it is possible to have separate matcher/datasets for the various systems and still use one instance of the ABIS. This ensures a stronger data separation but it still means that the application security of the ABIS has to be trusted.
Architectural option #4: Multiple ABIS, logically separated template data stores	±	A SIEM solution (log management, events correlation, alerts, dashboards, compliance, retention, forensic analysis) could be used to ensure secure logical separation and immediate detection even in case of malicious penetration (beyond virtual machine and logical firewalls). However, this does not apply for the database element within this option. Because all data is in the same database the risk increases that due to human configuration error data of CS 1 becomes visible to CS 2, or that record updates/deletes meant for CS 1 are also executed for system 2. It should be noted that the sensitivity of the records in the database is limited because no personal data and no biometric images are stored at ABIS level. Furthermore, a template can’t be reversed to the original fingerprint. The principle risk identified during study was that use of stolen data could enable identification of the fact that a particular person

		was potentially in that database – enabled through execution of a search on that data. However, because the NIST files (the files with the real FP) are not stored - only the template – this would furthermore require knowledge of and access to the algorithms used for template creation and matching.
Architectural option #5: Common ABIS, shared template database	-	eu-LISA would need to trust the IT security of ABIS system's "black box". The ABIS providers report their systems have limited built in application security. A separate impact assessment would be needed. Since all data resides on the same virtual network, one IT security or configuration issue could be sufficient to breach from e.g. SIS II to Eurodac data. Monitoring for these kind of breaches is far more difficult compared to the other scenarios, because it is not possible to rely on VM or network logging to detect breaches. For some vendors it is possible to have separate matcher/datasets for the various systems and still use one instance of the ABIS. This ensures a stronger data separation, but it still means that the application security of the ABIS has to be trusted. Because all data is in the same database (only separated by table or tag) the risk increases that due to a human configuration error, data of CS 1 could become visible to CS 2 or that record updates/deletes meant for CS 1 might also be executed for system 2 It should be noted that the sensitivity of the records in the database is limited because no personal data and no biometric images are stored at ABIS level. Furthermore, a template can't be reversed to the original fingerprint. The principle risk identified during study was that use of stolen data could enable identification of the fact that a particular person was potentially in that database – enabled through execution of a search on that data. However, because the NIST files (the files with the real FP) are not stored - only the template – this would furthermore require knowledge of and access to the algorithms used for template creation and matching.
Architectural option #6: Multiple ABIS, consequent logical separation of templates, highly flexible, eu-LISA governed	+	Logical separation of data is managed and ensured via the ABIS-orchestration-layer which would be fully managed by eu-LISA. Identity and Access Management could be partially accomplished at MS level – it would be up to the national system (NS) to authorize access to the systems. System design would nevertheless allow for a (future) full cascading of access through to the individual end-user if this became a requirement. Although the physical separation of data across servers is not foreseen, such an "air gapped" architecture seems not to be specifically required by applicable regulations, according to the interpretation of the legal framework in force. Consultations with data protection experts suggested

that logical data separation, if appropriately implemented, can be considered sufficient.

It should be noted that the sensitivity of the records in the database is limited because no personal data and no biometric images are stored at ABIS level. Furthermore, a template can't be reversed to the original fingerprint. The principle risk identified during study was that use of stolen data could enable identification of the fact that a particular person was potentially in that database – enabled through execution of a search on that data. However, because the NIST files (the files with the real FP) are not stored - only the template – this would furthermore require knowledge of and access to the algorithms used for template creation and matching.

2.3.2 Legal impact

Other aspects of the legal basis additional to IT security (mainly data protection), Business Continuity, performance and accuracy requirements that could potentially favour/ raise risks for any one of the proposed target state options have been considered as follows.

Architectural options	Score	Justification
Architectural Option #1: Fully separated architecture (continuation of AS-IS situation)	++	Considered in line with the consulted legal documentation for the existing and upcoming systems. No legally binding restrictions applicable to this proposed architectural option were identified, mainly since the systems are "air gapped".
Architectural Option #2: Multiple ABIS, templates in multiple data stores	+	Considered in line with the consulted legal documentation for the existing and upcoming systems. No legally binding restrictions applicable to this proposed architectural option were identified, mainly since the systems are logically separated from each other, and the ABIS provides the same functionalities and meets the same objectives related to output, cost-effectiveness, IT Security and quality of service.
Architectural Option #3: Common ABIS, logically separated template data stores	-	Considered in line with the consulted legal documentation for the existing and upcoming systems. No legally binding restrictions applicable to this proposed target architecture option were identified, However according to eu-LISA's Data Protection Officer, this option presents more risks than the previous two target state architecture options, mainly from a data protection (integrity and confidentiality) perspective, as one needs to trust the ABIS system's "black box". Each existing system (e.g. Eurodac, SIS II, VIS) is currently individually regulated, operated and monitored (data collection, transmission, data

		access, retention etc). Should a common ABIS be desired, the existing regulations would have to be updated.
Architectural Option #4: Multiple ABIS, logically separated template data stores	±	See Option #2. The considerations are identical with the exception of the shared storage at template level. New legislative provisions would probably be required to provide for such common storage.
Architectural Option #5: Common ABIS, shared biometrics data	-	See architectural option #3. The considerations are identical with the exception of the shared storage at template level. New legislative provisions would probably be required to provide for such common storage.
Architectural Option #6: Multiple ABIS, consequent logical separation of templates, highly flexible, eu-LISA governed	++	Considered to be in line with the consulted legal documentation for the existing and upcoming systems. No legally binding restrictions applicable to this proposed architectural option were identified, mainly since the systems are logically separated from each other. Additionally, the cSBSP provides at least the same functionalities and meets the same objectives related to output, cost-effectiveness, IT Security and quality of service as the current setup. The eu-LISA Data Protection Officer's concerns (integrity and confidentiality) noted under option 3 would be met by the "open design" (no black box) and an "end-to-end" governance by eu-LISA. Each existing system (e.g. Eurodac, SIS II, VIS) could be individually regulated, operated and monitored (data collection, transmission, data access, retention etc.). Within the cSBSP data privacy would be guaranteed by the open design of the AOL and the logical separation of its matchers.

2.3.3 Interoperability, Integration and Interconnectivity

In line with the future legal interoperability proposals, the architectural options were analysed against the following considerations linked to interoperability:

- Common repository: To what extent will the service be compatible with a possible common identity repository and enable the production and continuous maintenance of such a repository across multiple systems?
- Would the architecture make the implementation of the Common Identity Repository (CIR) easier?
- Component reuse

Evaluation of interconnectivity and integration possibilities, with a focus on:

- Use of an ESB or other integration platform options
- Member State or agency remote access options, defined as either 'Read only access only' OR 'Full Access'
- Possible change from the email interface of Eurodac into a web service.

Architectural Options	Score	Justification
Architectural Option #1: Fully separated architecture (continuation of AS-IS situation)	--	Because of a lack of inter-connection, Member States (MS) would be required to query across several ABIS simultaneously to produce combined results on one single screen. This would require implementation of a single search interface for every Member State. Eurodac could remain based on email services but also could, in the (near-) future, evolve towards web services. Note: Could potentially be improved via possibilities to further standardize the ABIS system by using the same software, versions, etc. which could result in improved interoperability.
Architectural Option #2: Multiple ABIS, templates in multiple data stores	-	Fully standardized, virtual (VMware) images are used, enabling better reuse. A common ESB is used and only needs to be created once. Eurodac could in the future evolve into a web service.
Architectural Option #3: Common ABIS, logically separated template data stores	+	This option involves development of a shared ABIS with a common logical repository of biometric data, but with data separation maintained. In this way, a maximum level of efficiency obtained as only one ABIS instance needs to be maintained. This single integrated database, storing only encrypted templates, would be easier to maintain. A common ESB is used and only needs to be created once. Eurodac could in the future evolve into a web service.
Architectural Option #4: Multiple ABIS, logically separated template data stores	±	According to this setup, use of fully standardized, virtual (VMware) images, would be anticipated, enabling optimal reuse possibilities. A single integrated database, storing only encrypted templates, is used and would be easier to maintain. A common ESB is used and only needs to be created once. Eurodac could in the future evolve into a web service.

Architectural Option #5: Common ABIS, shared template database	++	This option involves development of a shared ABIS with a common logical repository of biometric data, but with data separation maintained. In this way, a maximum level of efficiency obtained as only one ABIS instance needs to be maintained. A single integrated database, storing only encrypted templates, is used and would be easier to maintain. A common ESB is used and only needs to be created once. Eurodac could in the future evolve into a web service. When an MS needs to search through all databases, Read Only Access could be facilitated as a remote access option. In this scenario, it would be possible to create it in the backend. Having one database and one ABIS system (with multiple matchers) makes it easier to perform cross CS searches. However, this would require an effort to standardize the templates across the systems (the templates could be based on 1000PPI and 500PPI, flat or rolled etc.). Because the database does not contain personall data (that would complicate the security setup) it would not make the implementation of a CIR directly connected to the sBMS easier. It would be necessary to use the current Central Systems to perform a FP search .
Architectural Option #6: Multiple ABIS, consequent logical separation of templates, highly flexible, eu-LISA governed	++	The design would be completely virtualized and based on a homogeneous enterprise platform (i.e. Common Shared Infrastructure). This would lead to easier setup and a configuration that scales to the supporting infrastructure. The already virtualized components of the existing systems could be deployed and adjusted to the platform in their configuration (reuse). Reconfiguration efforts would already be directed to ensure compatibility with the newly-designed ABIS-Gateway. The ABIS-Gateway would need to be designed to accommodate all existing and future systems and ensure reliable and standardized communication with the underlying ABIS-Orchestration-Layer (AOL). The ABIS-Gateway, once created, would be reused in both legs of the envisioned A-A-setup and at BCU if so decided. It would ensure standardized communication between the specific systems and their potentially specific matching-engine-setups (business driven) and the underlying template repository, through the to-be-created ABIS-Orchestration-Layer (AOL). The AOL would ensure standardised (plug-in-design) connection of current or future matching-engines with its specific configuration and gallery . This would ensure easier future integration of new (and potentially innovative) biometric technologies and the possibility to introduce the concept of a “soft migration” (i.e. without significant impact on end users nor significant down time of the solution) in case of any given changes in matching engines. The AOL would already prepare for the potential introduction of a “one-stop-shop”-search (ESP) as it enables communication with all matching

engines provisioned and can incorporate the needed business logic to answer to searches from multiple perspectives without combining the templates stored and protected in their relevant galleries. Whether this functionality would be triggered from out of the specific business-system (EES, SIS II, etc.) in way of a front-end design or bypassing the existing business instances in way of a separate back-end design would be a question of choice and could even be realized in parallel.

Eurodac could in the future evolve into a web service

2.3.4 Scalability, Capacity and Performance

One of the criteria taken into account when analysing the architectural options was the efficiency with which the future system could be scaled. The main elements of this analysis were:

- Future potential capacity and performance changes (known and unknown)
- Identifiable bottlenecks that could trigger the need for capacity extensions, and estimated scalability
- Identification of the means required for an extension (hardware, software, etc.)
- Technical limit(s) or threshold(s) that could prevent any further extension of the proposed solution
- WAN bandwidth between Central Unit (CU) and Back-up Central Unit (BCU) (PtP/Point to Point)
- Load balancing requirements and virtualization possibilities.

Architectural Options	Score	Justification
Architectural Option #1: Fully separated architecture (continuation of AS-IS situation)	-	Can meet eu-LISA-specific scalability, capacity and performance requirements without considering efficiency (e.g. cost). Large ABIS vendors have existing 100 MIO+ fingerprint implementations, demonstrating possibilities in this regard. Server virtualization and active-active cluster architecture could be used to optimize capacity and HW usage of each system separately. Although it is equally possible to scale, more hardware (HW) resources would be needed to accomplish this architecture compared to the other four scenarios. In a growth scenario, this option requires more hardware components than the other four architectures. This means that the cost to scale is the highest in case of this option.
Architectural Option #2: Multiple ABIS, templates in multiple data stores	±	Can meet eu-LISA-specific scalability, capacity and performance requirements by partially considering efficiency. Server virtualization and active-active cluster architecture should be used to optimize capacity and HW usage of this option. All ABIS systems use the same physical hypervisors, thus resources are shared. When both production and pre-production environments use the same servers, less capacity is needed. In case of a data centre-wide incident, the pre-production systems could be switched off to ensure the production has sufficient capacity. This also results in less required hardware.

Architectural Option #3: Common ABIS, logically separated template data stores	++	Can meet eu-LISA-specific scalability, capacity and performance requirements. Server virtualization and active-active cluster architectures could be used to optimize capacity and HW usage of this option. The internal architecture of the common ABIS may limit capacity and performance if it does not properly support horizontal and vertical scaling. However, discussions with ABIS vendors within the sutyd indicated that this should not be a problem. This also means that the cost to scale is lowest in this option.
Architectural Option #4: Multiple ABIS, logically separated template data stores	+	Can meet eu-LISA-specific scalability, capacity and performance requirements. Server virtualization and active-active cluster architecture should be used to optimize capacity and HW usage of this option. All ABIS systems use the same physical hypervisors, thus resources are shared. When both production and pre-production environments use the same servers, less capacity is needed. In case of a data centre-wide incident, the pre-production systems can be switched off to ensure the production has sufficient capacity. This also results in less required hardware.
Architectural Option #5: Common ABIS, shared template database	+	Can meet eu-LISA-specific scalability, capacity and performance requirements. Server virtualization and active-active cluster architecture should be used to optimize capacity and HW usage of this option. The internal architecture of the common ABIS may limit the capacity and performance if it does not properly support horizontal and vertical scaling. However, discussions with ABIS vendors within the sutyd indicated that this should not be a problem. This also means that the cost to scale is lowest in this option.
Architectural Option #6: Multiple ABIS, consequent logical separation of templates, highly flexible, eu- LISA governed	++	Due to the infrastructure platform design, eu-LISA-specific scalability, capacity and performance requirements are met in all dimensions, including efficiency (e.g. cost). The potential merging of production and pre-production environments onto the same infrastructure-platform could significantly increase the resulting synergies in the basic design, as well as in incident-handling. This results from to the possibility to dynamically resize the environments to meet immediate operational needs. This could result in either significant savings in terms of less hardware being required or a significant gain in performance/capacity through use of the same dimension of hardware provisioning in addition to much more flexibility in incident-handling.

2.3.5 Business Continuity

Evaluation of availability and continuous operation possibilities, with a focus on:

- Operational business continuity (in terms of day-to-day operation of services), full or partial unavailability
- Strategic business continuity (in terms of capability to upgrade on the basis of market innovations/advanced technologies)

Architectural option	Score	Justification
Architectural Option #1: Fully separated architecture (continuation of AS-IS situation)	±	A higher availability level is possible and is independent of the target state architecture. It can be achieved by e.g. an active-active setup. There is potential for partial unavailability of single services without cross services/application impact.
Architectural Option #2: Multiple ABIS, templates in multiple data stores	-	A higher availability level is possible and is independent of the target state architecture. It can be achieved by e.g. an active-active setup. Within this option, if the ESB fails, all biometric services will be unavailable.
Architectural Option #3: Common ABIS, logically separated template data stores	--	A higher availability level is possible and is independent of the target state architecture. It can be achieved by e.g. an active-active setup. Within this option, if the ESB or ABIS fails, all biometric services will be unavailable. Additionally, if the database management system fails, all CUD (Create/Update/Delete) services will be down.
Architectural Option #4: Multiple ABIS, logically separated template data stores	+	A higher availability level is possible and is independent of the target state architecture. It can be achieved by e.g. an active-active setup. Within this option, if the ESB fails, all biometric services will be unavailable. Because of the separate ABIS systems, there is potential for partial unavailability of single services without cross services/application impact. The addition of the ESB and possible use of standardised ABIS images might allow for dynamic allocation of matching resources, boosting business continuity.
Architectural Option #5: Common ABIS, shared template database	+	A higher availability level is possible and is independent of the target state architecture. It can be achieved by e.g. an active-active setup. Within this option, if the ESB or ABIS fails, all biometric services will be unavailable. Nevertheless, the addition of the ESB and possible use of standardised ABIS images might allow for dynamic allocation of matching resources, boosting business continuity.
Architectural Option #6: Multiple ABIS, consequent logical	++(+)	Operational business continuity is well assured. With each of the Core Business Systems (CBS) running on the infrastructure platform, failing resources can be more easily replaced

separation of templates, highly flexible, eu-LISA governed

than in other cases, by redirecting existing resources of the platform. BCP's can foresee the highly automatized deployment of additional instances of any of the CBS to replace the failing structures. This flexibility could be greatly enhanced by combining the resources of production and pre-production environments into one platform.

The above holds true for any of the deployed matching engines. In addition, the exploit of existing technology could potentially enable the "semi-automatized" dynamic allocation of additional matchers or re-designating existing matchers of the same kind across systems in case of harmonization and respective utilization of the orchestration layer. Existing technologies for the administration of enterprise infrastructure platforms would significantly enhance eu-LISA's possibilities to make use of automatization in deployment, testing and maintenance by ensuring homogenized environmental conditions across all systems.

Strategic business continuity is also assured:

The implementation of the ABIS-Gateway, as well as the design of the cSBSP including its ABIS-orchestration layer (AOL) would dramatically increase eu-LISA's flexibility to encounter threats to its strategic business continuity:

- The possibility to at any time add or replace any type of matching engine (thereby terminating the vendor-lock-in threat)
- The possibility to add new matching technologies underneath the AOL (thereby opening the door to incorporating innovative technologies)
- Run old and new matching technologies in parallel for any given system (thereby enabling the method of soft-migration "out of" and "into" any desired changes within the matching-engine-domain, as operational or strategic needs may call for).

2.3.6 Flexibility

An evaluation of flexibility possibilities was carried out, with a focus on:

- List of standards compatible with proposed solution, and prospective accepted deviations
- Incompatibility details with existing implementations
- Application maintainability and extensibility
- Impact of changing vendors or vendor changes (possible agility across vendors and technologies)
- Ability to make changes to the ABIS triggered by a particular business domain without negative inter-services impact
- Automatized deployment of changes

Architectural Option	Score	Justification
Architectural Option #1: Fully separated architecture (continuation of AS-IS situation)	--	This air-gapped architecture allows for flexibility to implement changes without inter-service impacts. Nevertheless, it prevents agility for a timely and resource-efficient rollout of inter-services changes. As all systems are fully "air gapped", automatized deployment/ upgrades/ configuration changes are possible only within each ABIS solution.
Architectural Option #2: Multiple ABIS, templates in multiple data stores	±	Architectures based on logical separation, such as this, allow for flexibility to implement changes without inter-service impacts on the non-infrastructure layers. They also enable agility in the timely and resource-efficient rollout of inter-services changes and support the increasing need for interconnection/ interoperability. Architectures based on logical separation are capable of supporting automated deployment/ upgrades/ configuration changes. Option #2 only features a common ESB and the underlying shared infrastructure, limiting some aspects of flexibility. Note that there would be inter-service impact for any interventions related to the shared components.
Architectural Option #3: Common ABIS, logically separated template data stores	-	See Option #2 Option #3 features a common ESB, a common ABIS, a common database management system, in addition to the underlying shared infrastructure. Note that there would be inter-service impact for any interventions related to the shared components.
Architectural Option #4: Multiple ABIS, logically separated template data stores	+	Architectures based on logical separation, such as this, allow for flexibility to implement changes without inter-service impacts on the non-infrastructure layers. They also enable agility in the timely and resource-efficient rollout of inter-services changes and support the increasing need for interconnection/ interoperability. Architectures based on logical separation are capable of supporting automated deployment/ upgrades/ configuration changes. Note that there would be inter-service impact for any interventions related to the shared components.
Architectural Option #5: Common ABIS, shared template database	-	See Option #2 Option #5 features a common ESB, a common ABIS, a common database management system with one common data repository, in addition to the underlying shared infrastructure. Note that there would be inter-service impact for any interventions related to these shared components.

Architectural Option #6: Multiple ABIS, consequent logical separation of templates, highly flexible, eu- LISA governed	++(+)	Architectures based on logical separation allow for flexibility to implement changes without inter-service impacts on the non-infrastructure and “non-shared” layers. Architectures based on logical separation support agility for a timely and resource-efficient rollout of inter-services changes Architectures based on logical separation support the increasing need for interconnection/ interoperability. Architectures based on logical separation support are capable of supporting automated deployment/ upgrades/ configuration changes. In addition to the above, Option #6 features: • The possibility to enforce standardized interfaces on its standard building blocks to ensure easy replacement of outdated or obsolete parts - the ABIS-Gateways and the AOL are specifically designed to cover for this option • A built-in compatibility to future technology implementations, especially with respect to the matching engines ➤ Especially enabling eu-LISA to implement highly innovative technologies of new and agile vendors on the market as by design the system is not dependent on any particular technology and the incorporation of innovations does not pose any more strategic risk to the system ➤ Allowing for the consideration (tentative, without necessity of increasing risks) of smaller players in the market with economically interesting offers with less related operational or strategic risks • Application maintainability through a possible high degree of automatization based on the infrastructure platform design (Automatized deployment of changes) • A high degree of Application extensibility due to the infrastructure platform design and its implication to add and assign additional resources (“hot allocation” and “cold allocation”) • The least possible impact of a potential change in ABIS-vendors and the implicit change in vendor-technology • Potential agility to move across existing and upcoming new vendors and technologies • Ability to apply changes to any of the implemented matching engines triggered by a particular business domain without negative inter-services impact Inter-service impact for any interventions related to the shared
---	--------------	---

components

2.3.7 Others (Complexity of Implementation, Time to Market, Operations and Maintenance and Exit Scenarios – reversibility)

This segment of the evaluation focussed on other attributes, such as:

- Complexity of implementation
- Time to market for the initial implementation
- Time to market for future to be integrated systems utilizing the common shared biometric service platform
- Operations and maintenance
- Exit scenarios (reversibility)
- Potential to mitigate vendor lock-in
- Possible segmentation of the architecture to support innovations and use of multiple vendor technologies/solutions
- Embedded potential of the architecture to prevent inter-service impacts

Architecture Options	Score	Justification
Architectural Option #1: Fully separated architecture (continuation of AS-IS situation)	±	Low complexity of implementation (no migration needed) Short time to market for the initial implementation No significant change for operations and maintenance which has proven to be cumbersome and costly from a resource perspective in the past Easy exit scenarios (reversibility) Very limited potential to mitigate vendor lock-in within any business domain Major innovations are not supported by the architecture (long time-to-market, high resources, downtimes) No support for multiple vendor technologies solutions High embedded potential of the architecture to prevent inter-service impacts
Architectural Option #2: Multiple ABIS, templates in multiple data stores	-	Medium complexity of implementation (migration of existing systems needed) Medium time to market for the initial implementation Eases the complexity of operations and maintenance

		concerning the underlying infrastructure and the ESB, however introducing inter-service dependencies More complex exit scenarios (reversibility) than in case of option #1 Limited potential to mitigate vendor lock-in within any business domain Major innovations are not well supported by the architecture (long time-to-market, high resources, downtimes) No support for multiple vendor technologies solutions High embedded potential of the architecture to prevent inter-service impacts (except for the common shared infrastructure)
Architectural Option #3: Common ABIS, logically separated template data stores	--	High complexity of implementation (migration of existing systems needed) High time to market for the initial implementation Supports the option for integrated systems utilizing the common shared biometric service platform Eases the complexity of operations and maintenance concerning the underlying infrastructure, the ESB, the common ABIS and the common database management system, however introducing further inter-service dependencies More complex exit scenarios (reversibility) than in case of options #1 and #2 Increased potential for vendor lock-in Major innovations are not supported by the architecture (long time-to-market, high resources, downtimes) No support for multiple vendor technologies solutions Low potential of the architecture to prevent inter-service impacts
Architectural Option #4: Multiple ABIS, logically separated template data stores	-	High complexity of implementation (migration of existing systems needed) High time to market for the initial implementation Supports the option for integrated systems utilizing the common shared biometric service platform Eases the complexity of operations and maintenance concerning the underlying infrastructure, the ESB and the common database management system, however introducing further inter-service dependencies More complex exit scenarios (reversibility) than in case of options #1 and #2 Very limited potential to mitigate vendor lock-in within any business domain Major innovations are not supported by the architecture (long time-to-market, high resources, downtimes) No support for multiple vendor technologies solutions Medium embedded potential of the architecture to prevent inter-service impacts (except for the common shared

		infrastructure and the common database management system)
Architectural Option -- #5: Common ABIS, shared template database		Very high complexity of implementation (migration of existing systems needed) High time to market for the initial implementation Supports the option for integrated systems utilizing the common shared biometric service platform Eases the complexity of operations and maintenance concerning all layers Very complex exit scenarios (reversibility) Increased potential for vendor lock-in Major innovations are not supported by the architecture (long time-to-market, high resources, downtimes) No support for multiple vendor technologies solutions and potential of the architecture to prevent inter-service impacts
Architectural Option + #6: Multiple ABIS, consequent logical separation of templates, highly flexible, eu- LISA governed		High complexity of implementation (with special regards to the envisioned AOL) Longer time to market for the initial implementation Appears to be the optimal option for future integration of systems utilizing the common shared biometric service platform Significant ease of change for operations and maintenance once operational. Currently, such efforts can be cumbersome and costly, especially from a resource perspective, due to • the underlying infrastructure • the ABIS-Gateway • the ABIS-Orchestration-Layer • the Common Database Management System however introducing further inter-service dependencies. Innovations are highly supported by the architecture (very short time-to-market, comparably low expenditure in resources, no downtime, possibility for a "soft-migration") High support for multiple vendor technologies solutions (due to the implementation of the ABIS Orchestration Layer, new matching engines could be dynamically added and traffic re-directed towards them once they are up and running) Fairly high embedded potential of the architecture to prevent inter-service impacts.

2.3.8 Financial Impact

An initial high level financial analysis and estimation of key cost components was undertaken based mainly on the following costs:

- Implementation cost
- License costs
- Hardware costs
- Maintenance costs.

The costs were assessed per architectural option, as follows:

Architectural Option #1: Fully separated architecture (continuation of AS-IS situation)

No additional specific implementation costs are expected (unless an optimized virtual architecture is to be implemented).

Architectural Options #2/4: Multiple ABIS with templates in multiple data stores (logically or physically separated)

All systems in place at the time of development (EES, Eurodac, SIS II and VIS) will need to be configured and integrated again. Everything has to be retested in detail, but most of the configuration is expected to be reusable. Expected costs: 30% of initial implementation costs.

In a virtualized environment, the hardware costs are typically 30% lower compared to #1 (based on benchmark data).

Because most maintenance efforts could be shared with the other systems (and then deployed with limited differences for all environments) the expected effort is maximum of 25% of the current cost (based on 4 systems but it may further decrease by future systems to come). However, some extra governance and configuration changes have to be made, which will increase the costs by ~30%. The resulting costs are ~32% of the current costs.

Architectural Options #3/5: Common ABIS with multiple or a common template data store

In a common ABIS situation, only hardware and licenses can be reused (the implementation has to be redone completely). Furthermore, significant extra governance will be required to ensure that all requirements and their impact are understood and accepted by all stakeholders. The expected extra governance costs for this will be up to 50% higher than the initial one for existing implementation and available costs. However, because the implementation costs can be shared across a number of different systems, the resulting expected costs are: 37.5% (i.e. $150\% \times 25\%$) higher than the initial cost for the current BMS implementation.

All ABIS providers report that a common ABIS solution will be less expensive from a license perspective. Combined with the fact that less spare capacity is needed, a 20% lower license cost in case a shared biometric solution is deployed may be estimated.

Besides the lower hardware costs made possible by using virtualization (a 30% decrease in hardware costs is projected), even less servers are required because some servers (e.g. license and workflow) are needed only once (rather than 4 times in the case of 4 AFIS systems). The expected reduction in server costs is therefore 40%.

Architectural option #6: Multiple Matching-Engines with templates in multiple data stores (logically

separated)

All systems will need to be configured, automated and deployed again. Everything has to be retested in detail, but large quantities of the configuration could be expected to be reusable. Expected costs: 30% of initial implementation costs.

In a virtualized environment, the hardware costs are typically 30% lower as compared to the current, silo-ed physical architecture (based on benchmark data). An infrastructure without special appliances could significantly enhance this effect on general hardware and footprint in the Data Centre. This effect is estimated to be rising with the respective size of the overall environment.

Because most maintenance efforts can be shared with the other systems (and then deployed with limited differences for all environments) the expected effort is a maximum of 25% of the current cost (based on 4 systems but the “percentage share” may further decrease with future systems to come). However, some extra governance and configuration changes have to be made, which will increase the costs by ~30%. The resulting costs are ~32% of the current costs.

Implementation costs for development and implementation of the new AOL, the ABIS-Gateway together with the relevant business logic and interfaces to harmonize the communication interfaces of the existing systems towards the AOL still need further consideration. With this architecture, it is expected that eu-LISA would gain tremendous independence from any single vendor and the possibility to detach the organization from any significant change in licensing costs, if deemed economically necessary.

The general cost impacts are assessed in the following table. All proposed architectures should result in reduced costs over a 5-year period compared to the possible expansion of a current setup. Higher impacts marked in this table imply therefore more significant cost savings.

Target Architectural Option	Estimated costs impact, including implementation and 5 years running as sBMS	Overall Cost Impact
Current costs	Baseline	
Option #1: Fully separated architecture (continuation of AS-IS situation)	-40% compared to baseline	LOW
Option #2: Multiple ABIS, templates in multiple data store	-44% compared to baseline	MEDIUM
Option #3: Common ABIS, logically separated template data stores	-49% compared to baseline	HIGH
Option #4: Multiple ABIS, logically separated template data stores	-44% compared to baseline	MEDIUM

Option #5: Common ABIS, shared template database	-49% compared to baseline	HIGH
Option #6: "common Shared Biometric Service Platform (cSBSP) - Multiple matchers, logical separation of templates	-40% compared to baseline	LOW

2.3.9 Data Separation-Related Risks Overview

Eu-LISA has protected the current CBS's from security threats such as infections of custom malware, targeted hacking, malicious insider attacks, accidental exposure of sensitive data and simple software bugs. It is assumed that the security threats and the mitigation approaches of the target architecture options differ security-wise from each other only by how data separation is implemented. The following table shows an overview of the security assessment of the options from this perspective:

Architectural Options	Description of data separation	Risk level	Mitigation approaches
Architectural Option #1: Fully separated architecture (continuation of AS-IS situation)	Data separation is implemented physically	Low	All systems are air-gapped. Potential physical security-related risks e.g. human error, intrusion attacks/ threats, malicious data injection etc. persist.
Architectural Option #2: Multiple ABIS, templates in multiple data stores	ABIS users may share the same hypervisor, physical server, physical network and storage for their ABIS queries and data. Access is controlled for each individual user. There is a need for maintenance of separation of virtual ABIS instances and workloads.	Low	Isolation between virtual machine processes/data is assured Encryption may be provided for as an option. Decryption keys would only be provided to legitimate VM clones, hardening the virtualization layers Use of a SIEM solution to ensure immediate detection of malicious attacks would be possible
Architectural Option #3: Common ABIS, logically separated template data stores	ABIS users may share the same hypervisor, physical server, physical network and storage for their ABIS queries and data. Access is controlled for each individual user. There is a need for maintenance of separation between the parallel runtime services/ processes of the ABIS application.	Low – Medium	Same as above, plus - Data separation within the ABIS application would be provided for via a software-based tagging - Use of mandatory access controls and encryption for inter-process communication

	Configuration errors can expose the data stored in the templates databases to other CS users.		
Architectural Option #4: Multiple ABIS, logically separated template data stores	ABIS users may share the same hypervisor, physical server, physical network and storage for their ABIS queries and data. Access is controlled for each individual user. There is a need for maintenance of separation of virtual ABIS instances and workloads. Limited separation of data in the database. One configuration error can expose data to other CS users	Low – Medium	Isolation between virtual machine processes/data is assured. Encryption may be provided for as an option. Decryption keys would only be provided to legitimate VM clones, hardening the virtualization layers Use of a SIEM solution to ensure immediate detection of malicious attacks at ABIS level would be possible Deployment of fine grained logging and reporting at the database layer would be recommended.
Architectural Option #5: Common ABIS, shared template database	ABIS users may share the same hypervisor, physical server, physical network and storage for their ABIS queries and data. Access is controlled for each individual user. There is a need for maintenance of separation between the parallel runtime services/ processes of the ABIS application. Limited separation of data in the database. One configuration error can expose data to other CS users	Medium	Same as above, plus • Data separation within the ABIS application would be provided for via a software-based tagging • Use of mandatory access controls and encryption for inter-process communication • Deployment of fine grained logging and reporting at the database layer would be recommended.
Architectural Option #6: Multiple ABIS, consequent logical separation of templates, highly flexible, eu-LISA governed	ABIS users may share the same hypervisor, physical server, physical network and storage for their ABIS queries and data. Access can be controlled for each individual user. There is a need for maintenance of separation of virtual ABIS instances and workloads. Limited separation of data in the database. One configuration error can expose data to other CS users.	Low	Isolation between virtual machine processes/data is assured. Encryption may be provided for as an option. Decryption keys would only be provided to legitimate VM clones, hardening the virtualization layers Use of a SIEM solution to ensure immediate detection of malicious attacks would be possible. Deployment of fine grained logging and reporting at the database layer would be recommended. The ABIS-Orchestration Layer could be of open design, transparent to eu-LISA and fully in its governance.

2.3.10 Summary of Comparison and Ranking

Criteria	Architectural Option #1: Fully separated architecture (continuation of AS-IS situation)	Architectural Option #2: Multiple ABIS, templates in multiple data stores	Architectural Option #3: Common ABIS, logically separated template data stores	Architectural Option #4: Multiple ABIS, logically separated template data stores	Architectural Option #5: Common ABIS, shared template database	Architectural Option #6: Multiple ABIS, logically separated, highly flexible, eu-LISA governed
3.2 IT security and compliance (integrity and confidentiality)	++	+	±	±	-	+
3.3 Legal impact	++	+	-	±	-	++
3.4 Integration and interconnectivity	--	-	+	±	++	++
3.5 Scalability, capacity and performance	-	±f	++	+	+	++
3.6 Business Continuity	-	±	++	+	++	++(+)
3.7 Flexibility	--	±	-	+	-	++(+)
3.8 Others (Complexity of implementation, Time to market, Operations and maintenance, Exit scenarios (reversibility))	±	-	--	-	--	+
3.9 Financial Impact	-	±	+	±	+	-
FLAT score summary	-3	0	2	2	1	4

3. Migration Options

3.1 Overview

The following section provides an overview of possible approaches of migrating from the as-is situation to the proposed to-be situation of having an operational shared biometric matching service for all eu-LISA large-scale IT systems. The section takes a generic look at migration options – considerations specific to any particular architectural option or set of options outlined in section 2 are highlighted where necessary. The specific impacts of various migration options on the enterprise are assessed.

Given the high risk level for eu-LISA, a big bang migration approach (where EES, SIS II, VIS etc. have the same migration date) is considered not feasible and has thus been excluded. A migration path where an “in between” situation is used to speed up the process of bringing a new application live is also not considered: it would require extra migration effort and has extra risks and costs. The only benefit of this could be the quicker initial implementation that might be possible if the use of the common ABIS is not mandatory. Yet since it is anticipated that such use will have to be mandatory in the long run (in order to realise the main objectives), it would make the process more complicated and therefore costly and is therefore discounted.

Two migration scenarios have been defined, namely:

- Option #1: Gradually enhance and reuse
- Option #2: Common Shared Infrastructure- Start in new environment

3.2 Analysis and Impact Assessment

Option #1: Gradually enhance and reuse

Characteristics	Considerations per architectural option
Option derived from the consideration that the hardware in use will still be part of standard and system specific Maintenance in Working Order contracts currently operating in the Agency. It is based on gradually enhancing and re-using the current hardware by creating a new virtual machine (VM) with the right setup (standardized), and then shutting down the physical or old VM with the same setup. Subsequently, the required changes in Pre-Production (Pre-PRD) would be made, followed by execution in Production (PRD). Noting that SIS II is built on a newer system with additional functionality compared to VIS-BMS 2.0,	Architectural Option #1 *: Duplicate the environment to a new platform to use as a basis for a new system (e.g. EES, Eurodac, SIS II) and migrate the data when needed. A communication layer in between both instances of Eurodac is a prerequisite for the full migration period to ensure the synchronization of the old and new template database (from old to new vendor). Architectural Options #2 - #5: Ensure the current environment is ready to serve multiple systems. An ESB has to be made ready for this (Access Management to support multiple systems), and the matchers and the workflow engines have to be

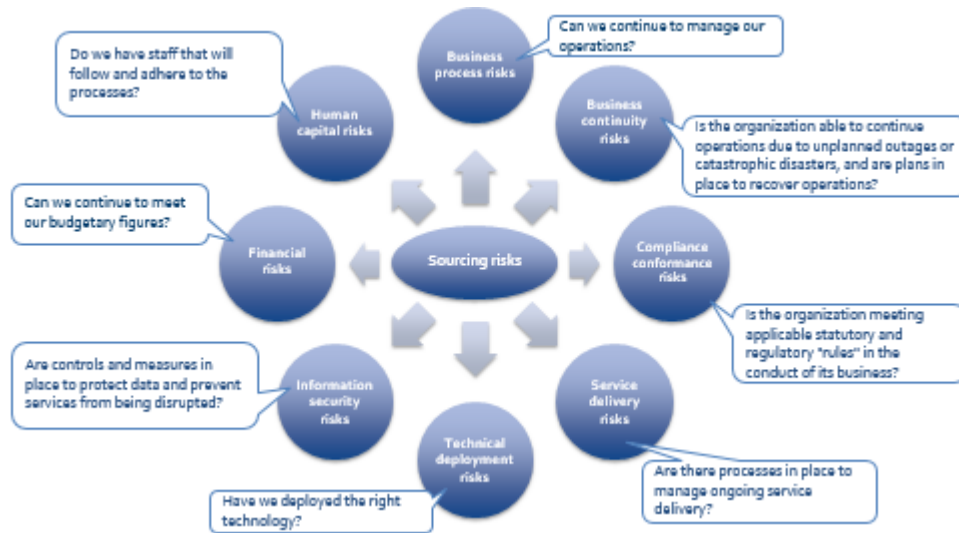
the sBMS could be built on SIS II, in which case no data migration would be needed for SIS II - the same underlying database would be used. It would be important to ensure that technology standards are used for search, identification, and latent search so that standard matcher images could be used for the pre-defined use cases. This would also ensure that the design is ready to support multi-modal Biometrics.	connected to the correct databases. Architectural Options #2* and #4*: Use of one matcher only for one dataset is necessary. When the setup is ready for multiple systems, it would be proposed to start migrating the data and ensure that both the old and the new system stay operational (where applicable) and fully functional for a period of time (estimated 3 months)
--	---

Option # 2: Common Shared Infrastructure - Start in new environment

Characteristics	Considerations per target state architecture option
Start from Common Shared Infrastructure (CSI) currently being developed by eu-LISA – the approach is based on duplicating the current (most advanced) configurations where possible (sometimes limited optimizations can be required due to changed CPU/Memory setup in the new environment; to eu-LISA's current knowledge this would be the case). It would be necessary to ensure that technology standards are used for search, identification, and latent search so that standard matcher images could be used for the pre-defined use cases. This would also ensure that the design is ready to support multi-modal Biometrics. Notably, efforts would have to be made to migrate all data while keeping the current systems up and running. It might be proposed to start with the system with the smallest and simplest setup (system to be decided) and migrate it to the new environment, before continuing to migrate the other systems in order of system complexity.	Architectural Option #1: N/A Architectural Option #2 - #5: Duplicate the environment to a new platform to use as a basis to build up the old and new systems. Architectural Options #2 - #6: Ensure both the old and the new platform are operational, but not necessarily at the same time, in order to reduce/mitigate potential migration risks Architectural Options #2 - #5: Ensure the current environment is ready to serve multiple systems. The ESB has to be made ready for this. Architectural Options #2 - #4: The matchers and the workflow engines have to be connected to the correct databases. Use of just one matcher per dataset is possible.

3.2.1 Impact Assessment Framework and Methodology

Migration options were assessed using eight evaluation categories that, when analysed together, provide a comprehensive overview of the risks associated with the chosen strategy.



Risk category	Topic covered	Impact description
Business process risks	Business Impact	Impact on eu-LISA's selected existing and upcoming systems (ECRIS-TCN, EES, Eurodac, SIS II and VIS) users, the Member States and external agencies.
Business continuity risks	Covered in Architecture Assessment	
Compliance conformance risks	Legal impact	Assessment of the legal (legally binding considerations and end users buy in) impact for each migration option.
Service delivery risks	Operational Impact	Impact on eu-LISA systems (ECRIS-TCN, EES, Eurodac, SIS II and VIS) operational processes and personnel
Technical deployment risks	Technical Impact	Impact on eu-LISA systems (ECRIS-TCN, EES, Eurodac, SIS II and VIS) performance and accuracy, as well as impact on network bandwidth consumption.
Information security risks	Covered in Architectural Options	

Financial risks	Financial Impact	Financial impact on eu-LISA's selected existing and upcoming eu-LISA systems, including justification of calculation rules and origin of the financial figures.
Human capital risks	Operational Impact	Impact on eu-LISA systems' (ECRIS-TCN, EES, Eurodac, SIS II and VIS) operational processes and personnel

3.2.2 Legal Impact

Migration option	Impact	Justification
Option #1: Gradually enhance and reuse	LOW	Since each existing system (e.g. Eurodac, SIS II, VIS) is individually regulated, operated and monitored (data collection, transmission, data access, retention etc), the legally binding documentation for existing and upcoming systems might need to be updated in line with the chosen Target State Architectural Option for the Common ABIS. A dedicated legal framework for the migration from the current state to the chosen Target State Architecture Option for the Common ABIS, in line with the chosen Migration Option needs to be created and approved by all end users (Member States and external agencies).
Option #2: Common Shared Infrastructure-Start in new environment	LOW	Same considerations as for Option #1. The appropriate basis for Common Shared Infrastructure, including the alignment of the existing systems and agreement upon shared common services requirements for all the existing/ upcoming systems within the sBMS etc. will need to be created and approved by all end users (Member States and external agencies)

3.2.3 Business Impact

Migration option	Impact	Justification
Option #1: Gradually enhance and reuse	LOW	No big bang approach is proposed nor any single migration effort recommended - gradual enhancements and reuse are the basis for this setup. If the SIS II BMS is used as the basis, the impact would be bigger for Eurodac, and vice versa. Since the Member States own the biometric data stored in the data centre (DC) in Strasbourg, they have both the authority and authorization to conduct acceptance tests and would thus have to be highly involved in performance and accuracy testing for major upgrades to ABIS systems in use/ new ABIS systems. The hardware in use will still be part of the MWO until the shared common services requirements for these systems matures and the existing/ upcoming systems will be sufficiently aligned. For sBMS, the selected Architectural Option and Migration Option, a dedicated testing methodology needs to be created and approved by eu-LISA in collaboration with its end users (Member States and external agencies) with clear RASCI (R – Responsible; A - Accountable (also Approver) ; S – Support; C – Consulted; I – Informed) responsibility matrix in place for eu-LISA, Member States, Member States and contractors, and vendors and any other relevant stakeholders to ensure a transparent distribution of all migration mitigation and planning activities.
Option #2: Common Shared Infrastructure- Start in new environment	LOW	Similar considerations as for Option #1. When migrating directly to the CSI, additional assurance needs to be given to end users that if in the short term there might be space issues within the current DCs (CU, BCU), it will not be the case in the long term, provided the existing systems' migration to the sBMS is done incrementally (one system at a time).

3.2.4 Financial Impact

Migration option	Impact	Justification
Option #1: Gradually enhance and reuse	MEDIUM	Limited new hardware is needed in the short term as current hardware used for physical servers might be re-useable for running VMs. While not the most efficient option, it may be (capex wise) cost effective in the short term. In the long term, more powerful physical servers would likely have to be used. This option will require a new migration in the relative short term and is assessed therefore as less cost effective in the longer term. Due to its gradual approach, the test effort and costs are relatively low (many simple tests are typically easier to coordinate compared to one big) The required training effort is low because no new ABIS is needed for most internal personnel (except for those used to working with systems potentially quite different from that re-used – inevitable given the variability of currently deployed AFIS systems). Although some extra personnel will need to be hired to backfill the current personnel (who will be involved in the migration, and have therefore less time for support) the number of extra staff is expected to be limited because the staff is already knowledgeable with the current ABIS.
Option #2: Common Shared Infrastructure- Start in new environment	LOW	Although new hardware is needed in the short term, this hardware should be part of the CSI infrastructure. Therefore upfront investments in hardware would not be needed as all costs be allocated using a cloud like model where only the usage is billed. This will obviously have an impact on the CSI budget and hardware requirements, nevertheless. Compared to Option #1, only one migration has to be performed. Even though the test effort might be more complex to organize, the expected total effort is expected to be lower. The required training effort is low, because no new ABIS is needed for most internal personnel (except for those used to working with systems potentially quite different from that re-used – inevitable given the variability of currently deployed AFIS systems). Although some extra personnel will need to be hired to backfill the current personnel (who will be involved in the migration, and have therefore less time for support) the number of extra staff is expected to be limited, because the staff is already knowledgeable with the current ABIS.

3.2.5 Technical Impact

Migration option	Impact	Justification
Option #1: Gradually enhance and reuse	MEDIUM	Although relatively simple to accomplish the migration according to this approach in the short term, due to the possibility to reuse components and the current replacement of the physical servers and virtualization (due to hardware being obsolete and due to contractual issues), this approach is not ready for the future CSI, resulting in the likely need for an additional migration in the (near-) future towards this new platform. It is not feasible to use pre-PRD for migration purposes to save infrastructure costs since it is already used for other activities (business continuity tests, major roll outs etc.) and since the target platform is CSI.
Option #2: Common Shared Infrastructure-Start in new environment	MEDIUM	Same considerations as for Option #1. As old and new systems would both be available in the beginning, the new sBMS system, tested in detail before go-live, could still be switched off and a reversion made after go-live to the old system if there is an issue (fall-back scenario). All existing systems in scope would have to align with the CSI solution and migrate to it eventually. However, the hardware in use in this migration scenario would still be part of the MWO until the shared common services requirements for these systems mature and the existing/ upcoming systems will be sufficiently aligned, imposing significantly more effort on the end users to properly test before going into PRD. There might be space issues within eu-LISA data centres (CU, BCU), at least in the shorter term. A solution needs to be identified for the BCU in particular.

3.2.6 Operational Impact

Migration option	Impact	Motivation
Option #1: Gradually enhance and reuse	MEDIUM	Some retraining is required for the current internal operational hands on eu-LISA ABIS experts, although the staff is already knowledgeable with the current ABIS. Due to the high levels of similarity and reuse, relatively few eu-LISA experts (number of missing staff to be determined based on impact on daily operations) are needed from the Production Application Support (PAS) sector to support the migration and implementation projects. Additional resources would be temporarily needed to support the Common

ABIS initiative from eu-LISA's main operations departments e.g. Border System Management Sector (VIS), Internal Security System Sector (SIS II), Asylum Sector (Eurodac), Test Sector, Security Sector, Network Sector, Infra Sector etc. In the long term (after the implementation) these new resources could help to support the 'to be' implemented systems.		
Option #2: Common Shared Infrastructure- Start in new environment	MEDIUM	Same considerations as for Option #1. When migrating directly to the CSI, additional staff would need to be involved to properly plan the migration activities and conduct a minute planning for the migration to the CSI platform. Additional assurance needs to be given to end users regarding the feasibility of such a migration to get their buy-in, resulting in additional effort in terms of communication by the eu-LISA staff.

3.2.7 Impact Assessment Results

Criteria	Option #1: Gradually enhance and reuse	Option #2: Common Shared Infrastructure- Start in new environment
Legal impact	LOW	LOW
Business impact	LOW	LOW
Financial impact	MEDIUM	LOW
Technical impact	MEDIUM	MEDIUM
Operational impact	MEDIUM	MEDIUM

Impact:

LOW	Low impact: Considerable effort and activities to be defined and planned to ensure a smooth migration and implementation of the common ABIS
MEDIUM	Medium impact: Significant effort and activities to be defined and planned to ensure a smooth migration and implementation of the common ABIS
HIGH	High impact: Major effort and activities to be defined and planned to ensure a smooth migration and implementation of the common ABIS

3.2.8 General Remarks Towards the Migration Options

In any of the envisioned migration options and across all reviewed Target State Options (1-6), a synchronization mechanism needs to be built to ensure the synchronization of the "initial" biometric database and the "target state" biometric database.

In Architectural Option 6, this mechanism is architecturally foreseen to remain in operation as this task would be done by the "ABIS Orchestration Layer".

Thus, it may be noted that Option 6 is the only option in which this significant investment will not be lost. On the contrary, the element would remain as a crucial piece of architectural design serving to achieve operational and strategical goals in a future-proof manner.

4. Flagging Functionality

4.1 Options Overview

Use Cases for Flagging (*Generic Flow*):

- A person who is the subject of a check can be registered in several systems simultaneously — potentially under different identities — given the specific purpose of each system
- Public authorities should be able to obtain reliable and up-to-date information about the status of such persons on the basis of possible matches from all relevant EU systems
- The Flagging search shall respect the original data access control of the parent system and the need to comply with data protection principles and the requirements of necessity, proportionality, purpose limitation and quality of data
- These hit/no-hit flags would not contain any specific data. They merely indicate the possibility of finding specific data, on the person in question, in another system.

Initially, the Flagging Use Cases should ideally use System to System Interfaces (S2S), as they are easier to use for the End-Users in the Member States. However, when the volume of Flagging requests is low, the Member States could also choose to use dedicated User Interfaces (User to Systems – U2S, which may also be provided centrally by eu-LISA), as they would not require changes to Member States National SSIs. It may be expected to make the consumption of the Flagging service easier in terms of effort required to invoke it.

Three non-exhaustive **Flagging Use Cases** have been identified, detailed, discussed and agreed upon for the scope of this report:

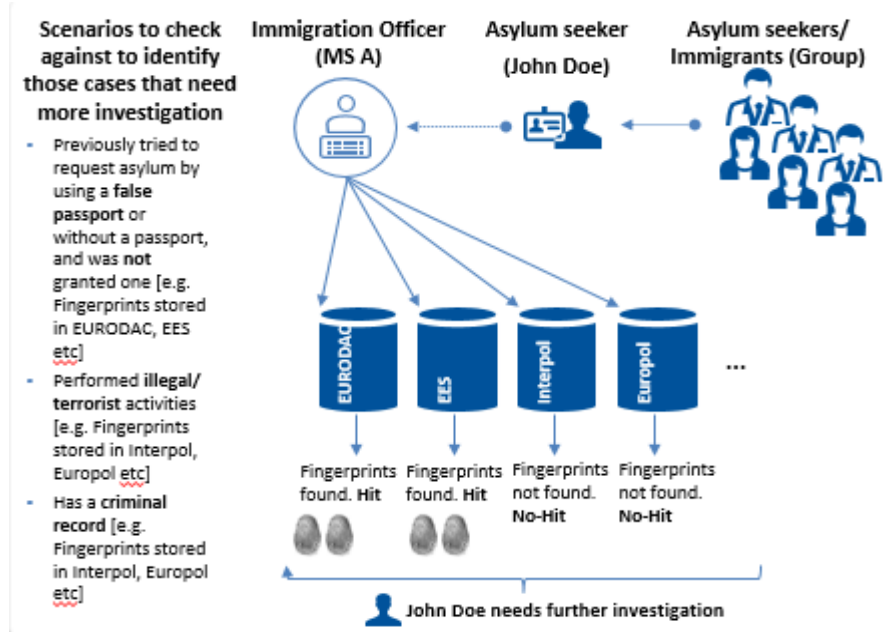
- Asylum - Immigration Hot-spot
- Law Enforcement - Law enforcement investigation: for complete and partial sets of Biometrics Data
- Border Control - Visa Application Examination.

Note: The Member States might later have to examine an additional workflow around the Flagging Process to cover the situation when the biometrics search with Flagging results in multiple flags/ hits, to be escalated and investigated by a person who has access to all the flagged Central Systems. In case different person hits result from a biometrics search with Flagging, a biometrics expert must be involved before the Flagging results incur any legal consequences e.g. applicant visa refusal.

Asylum - Immigration Hot-spot

An immigration officer in a MS, the End-User, needs to screen large numbers of Immigrants/ Asylum Seekers. The immigration officer thus needs to be able to rapidly search against multiple CSs on the basis of a Hit/No-Hit per CS to identify those cases that need more investigation.

- When applicable, the Flag Search request triggers Silent Notification(s) (e.g. SIRENE in SIS II) to the data owners, and reports No-Hit to the End-User.

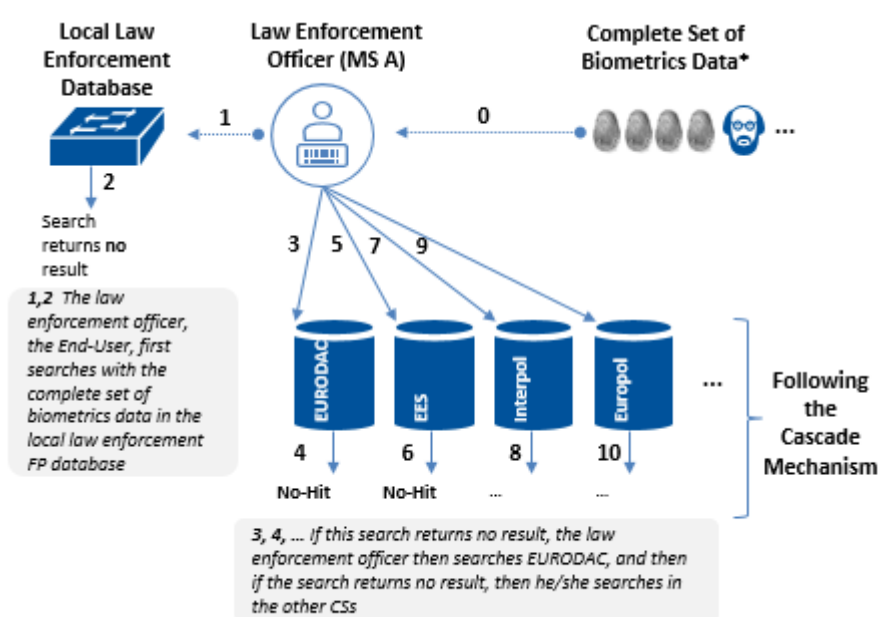


Law Enforcement - Law enforcement investigation

➤ For Complete Set of Biometrics Data

The law enforcement officer, the End-User, obtained a complete set of biometrics data and wants to see whether the complete biometrics data set is known in another CS.

- When applicable, the Flag Search request triggers (a) Silent Notification(s) (e.g. SIRENE in SIS II) to the data owner, and reports No-Hit to the End-User.
- When transactions are initiated for Law Enforcement purposes, the legal provisions applicable to current CSs provide for a "Cascade Mechanism" whose general idea is to extend the scope of searches progressively from police information systems to border control systems following a pre-established sequence and sometimes dependent on additional authorizations.

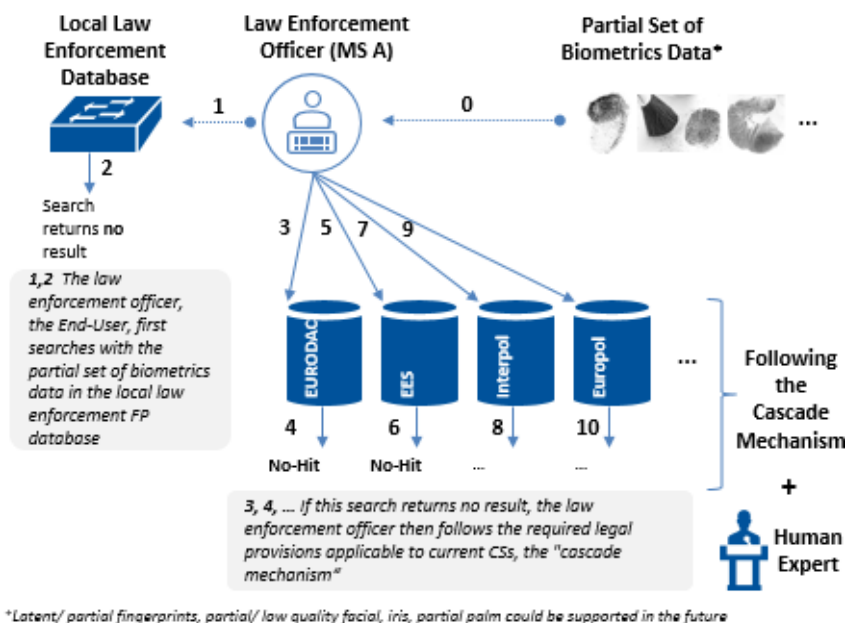


*Fingerprints, facial, iris, palm could be supported in the future

➤ **For Partial Set of Biometrics Data* including human expert involvement (Future)**

The law enforcement officer, the End-User, found a partial set of biometrics data and wants to see whether the partial set of biometrics data is known in another CS.

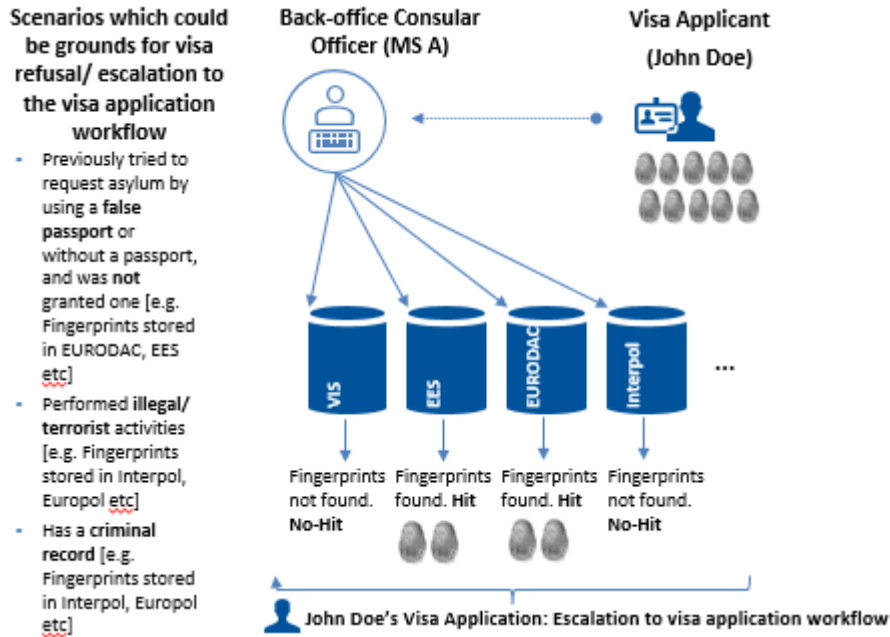
- When applicable, the Flag Search request triggers Silent Notification(s) (e.g. SIRENE in SIS II) to the data owners and reports No-Hit to the End-User.
- When transactions are initiated for Law Enforcement purposes, the general idea is to extend the scope of searches progressively from police information systems to border control systems following a pre-established sequence and sometimes dependent on additional authorizations.
- **Due to the nature of partial searches and potential low accuracy response rates, the involvement of a human expert is mandatory.**



Border Control - Visa Application Examination

In the normal visa application examination process, the MS back-office consular official checks the submitted documentation and when needed puts the FPs of the applicant in VIS. In an **enhanced** visa examination process, the MS back-office consular official also checks whether the applicant's e.g. FPs are already in any of the other databases.

- A retrieval in VIS and a FP search in SIS and other CSs are conducted in parallel.
- The End-User, MS back-office consular official, aims to check whether the person matches any of the scenarios which could be grounds for refusal/ escalation to the visa application workflow.
- When applicable, the Flag Search request triggers Silent Notification(s) (e.g. SIRENE in SIS II) to the data owners and reports No-Hit to the End-User.



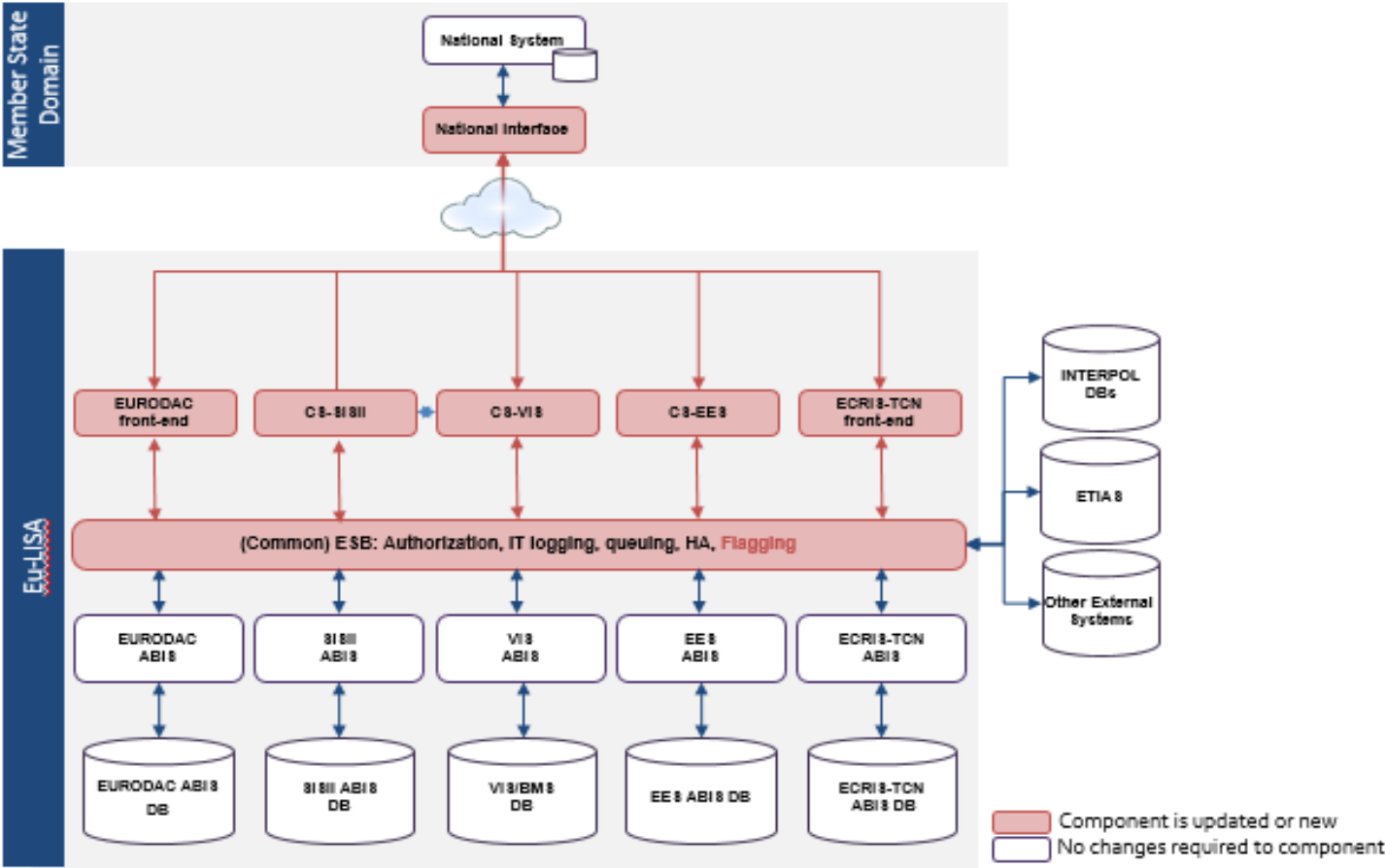
The Flagging Options have been defined primarily considering:

- The previously retained architectural options and analysis
- Possibilities to re-use the common ESB of the Shared BMS, which needs to undergo changes
- Limiting the number and impact of the changes needed for the CSs, ICDs, and the Member States
- Possibilities to embed the Flagging functionality in the European Search Portal (ESP)
- Possibilities to integrate with the Common Identity Repository (CIR)

4.2 Description

The following Flagging Options have been identified, defined and agreed upon with the main stakeholders of eu-LISA's working team:

Flagging Option 1: Common ESB handles Flagging

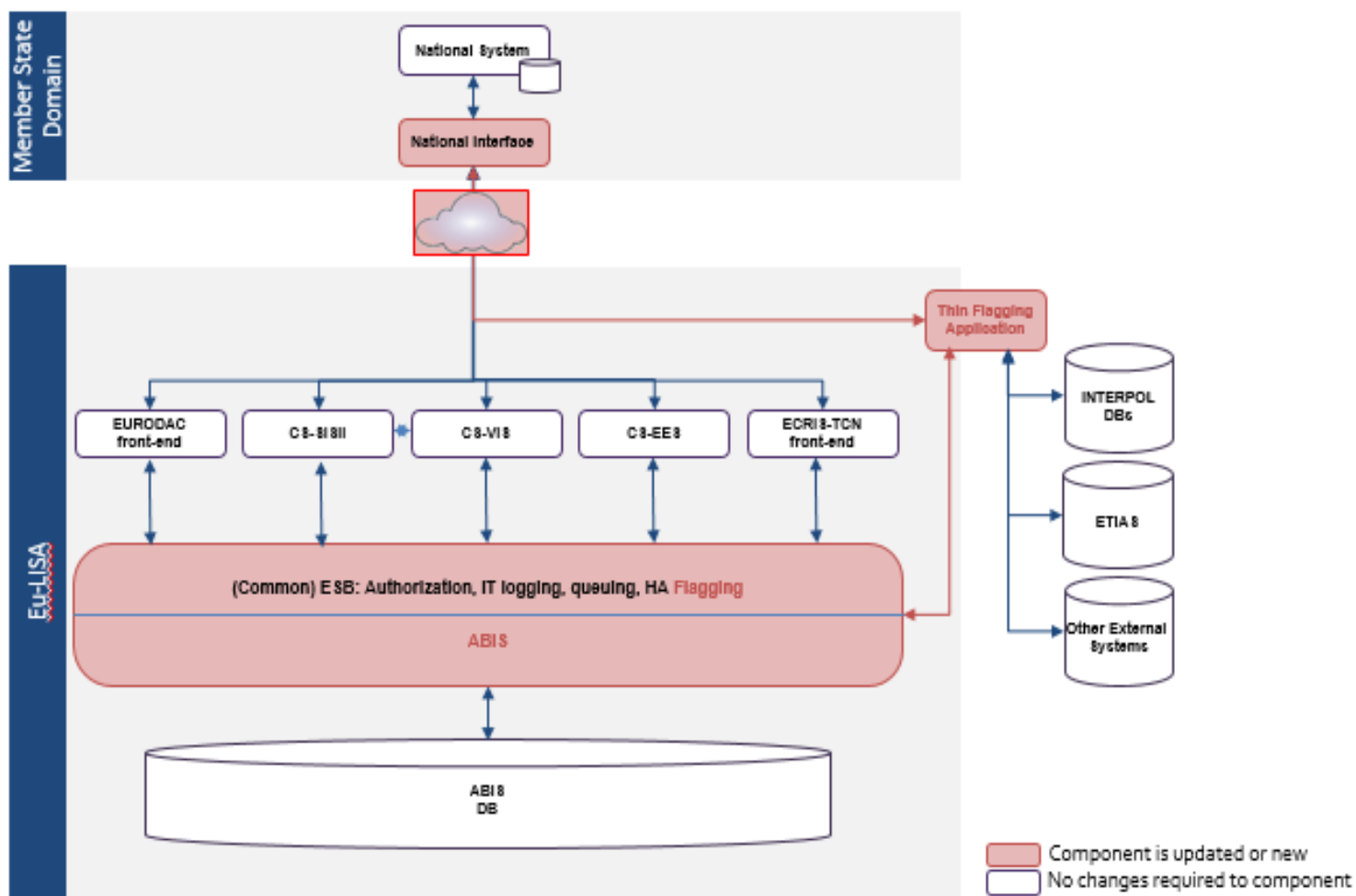


High-level application architecture considerations

Area/ Changes	MS National Interface (SSI)	Network	CSs	ESB	ABISs/ ABIS DBs	Others
Component is updated or new	- MS need to change their National Interfaces to make Flagging visible - All the MS-CS interfaces need to change, because all CSs can now return Flagging information for the other CSs	N/A	All CSs have to change, because they all need to be able to authenticate the "Flagging Only" request and to be able to sent this new request to the ESB, and then return the result to the MS	- The ESB will have to perform non-core ESB tasks e.g. sending one message to all CSs and wait for all responses before replying to the MS - The queries to the ABIS system need to be created by the ESB which is duplicated functionality, as this is also done in the CSs	N/A	N/A
No changes required to component	N/A		N/A	N/A		N/A

*The alternative is that the ESB sends the message to the CS, but in this case the CS needs to be changed in such a way that it is aware that results of the queries originating from the EBS will have to be returned to the ESB. This will require an additional ICD, and will make the setup very complex and error prone

Flagging Option 2: Common ESB and Single Instance Shared BMS Handles Flagging

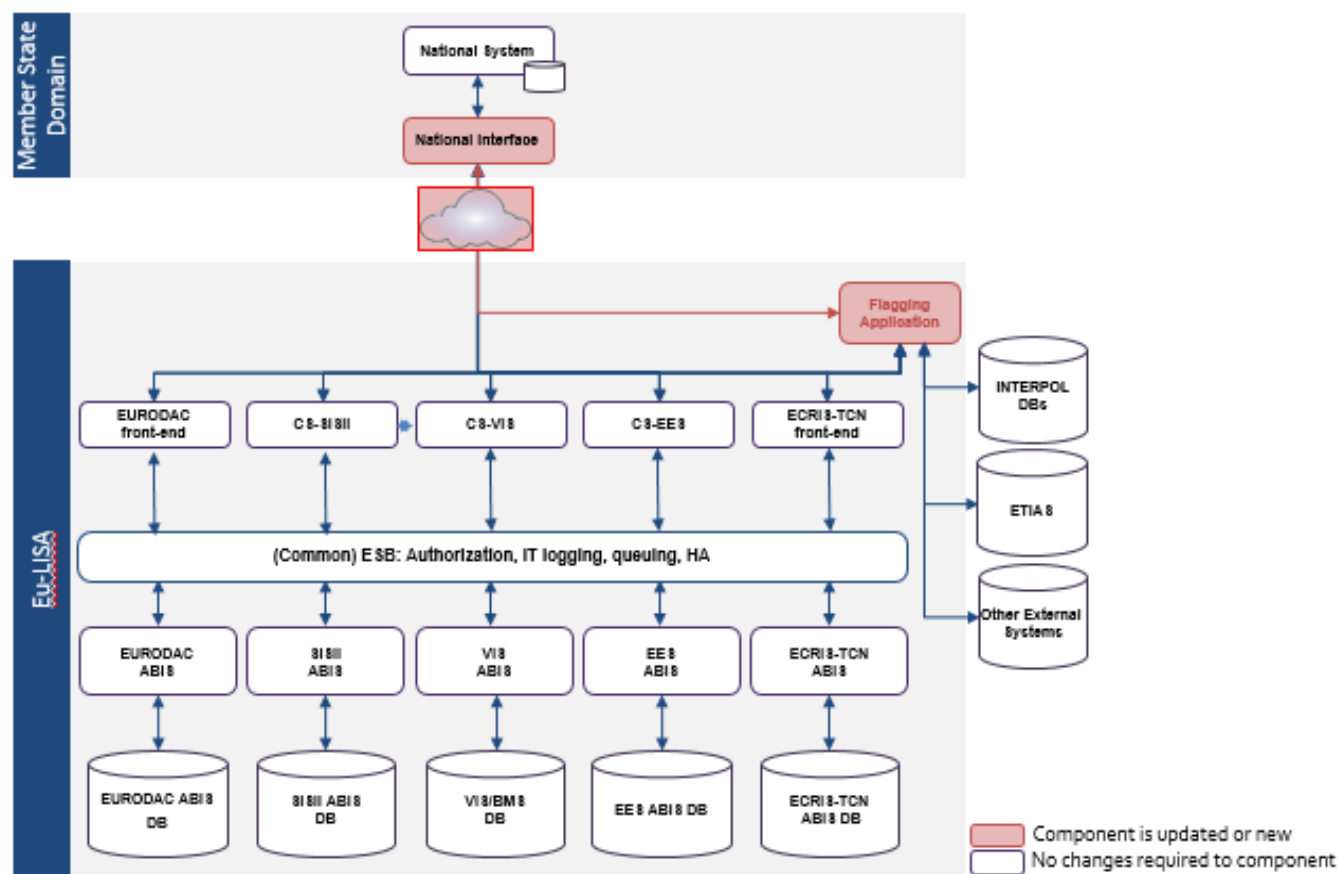


High-level application architecture considerations

Area/ Changes	MS National Interface (SSI)	Network	CSs	ESB	ABISs/ ABIS DBs	Others
Component is updated or new	- MSs have to change their National SSIs - The SSI needs to be able to make two requests: (1) the normal search request, and (2) the Flagging request	No changes required for the ICDs (additions only)	N/A	- The queries to the ABIS system need to be created by the ESB which is duplicated functionality, as this is also done in the CSs* - The ESB will have to perform non-core ESB tasks e.g. sending 1 message to all CSs and wait for all responses before replying to the MS	When using 1 ABIS DB it is possible to ensure that the ABIS solution handles Flagging	New Thin Flagging Application This app performs authorization of the request, and lets the ESB/ABIS do the flagging itself. Ensures the CS and the ICD's do not have to change for normal operation
No changes required to component	N/A	N/A	-	N/A		N/A

*The alternative is that the ESB sends the message to the CS, but in this case the CS needs to be changed in such a way that it is aware that results of the queries originating from the EBS will have to be returned to the ESB. This will require an additional ICD, and will make the setup very complex and error prone

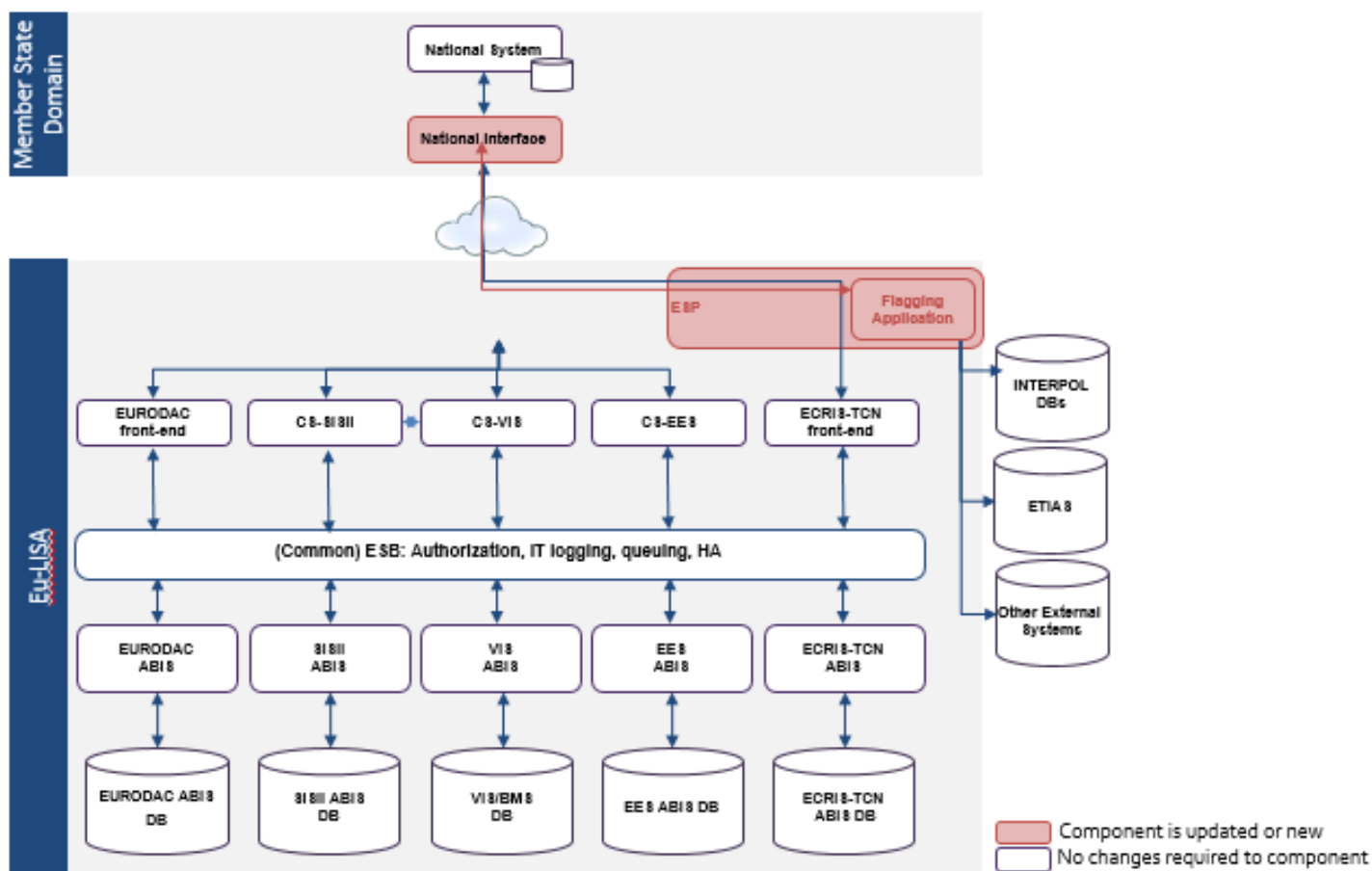
Flagging Option 3: Extra application which handles Flagging



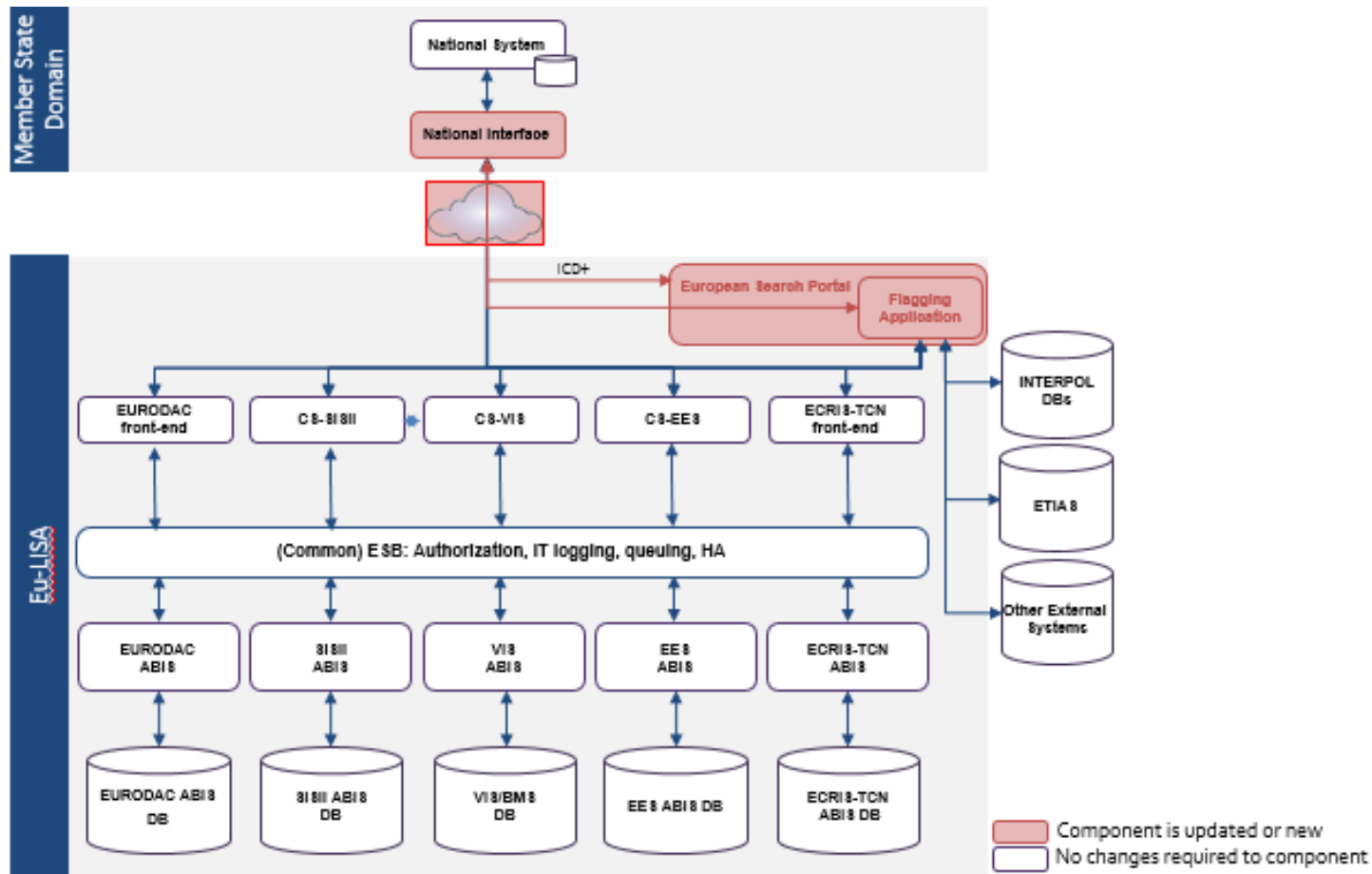
High-level application architecture considerations

Area/ Changes	MS National Interface (SSI)	Network	CSs	ESB	ABISS/ ABIS DBs	Others
Component is updated or new	- MSs have to change their National SSIs - The SSI needs to be able to make two requests: (1) the normal search request, and (2) the Flagging request	The Flagging Application needs to be able to connect to all CSs	N/A	N/A	N/A	New Flagging Application. The Flagging front-end will handle the authorizations, and will use the current CS to query the data
No changes required to component	N/A	N/A				

Flagging Option 4: Extra Search and Flagging Orchestrator layer



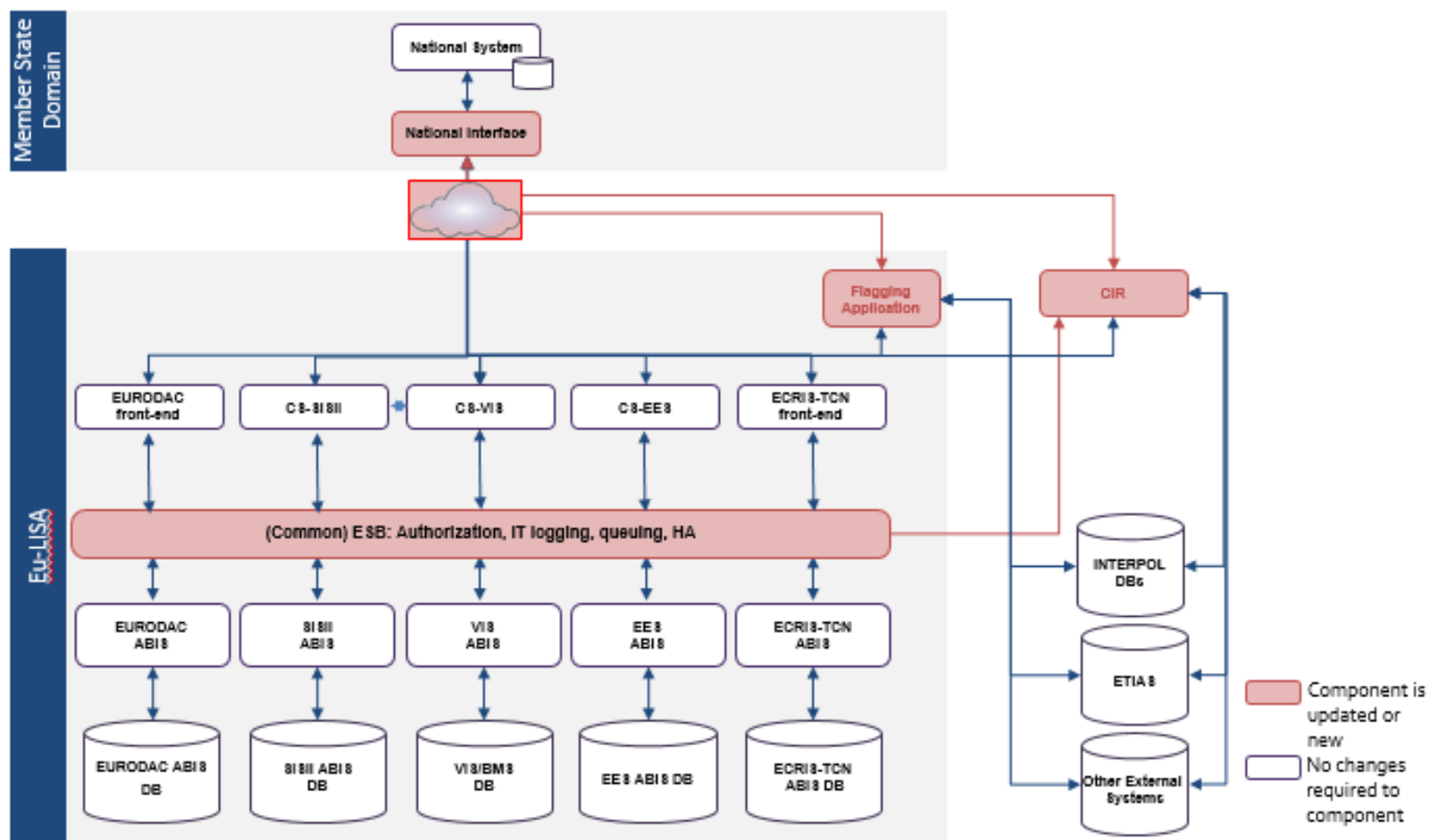
Flagging Option 4+: Extra Search and Flagging Orchestrator layer (European Search Portal)



High-level application architecture considerations

Area/ Changes	MS National Interface (SSI)	Network	CSs	ESB	ABISs/ ABIS DBs	Others
Component is updated or new	- MSs need to change their National Interfaces to make Flagging visible - All the MS-CS interfaces need to change, because all CSs can now return Flagging information for the other CSs	The Flagging Orchestration layer needs to be able to connect to all CSs	N/A	N/A	N/A	- New Search and Flagging Orchestrator layer. The interface between the Orchestrator and the CSs uses the current ICDs - Ensure that different SLAs are used for Normal Search (existing SLAs between the CS and the ABIS) versus Search which includes Flagging
No changes required to component	N/A	N/A				N/A

Flagging Option 5: Extra application which handles Flagging with CIR integration



High-level application architecture considerations

Area/ Changes	MS National Interface (SSI)	Network	CSs	ESB	ABISs/ ABIS DBs	Others
Component is updated or new	- MSs have to change their National SSIs - The SSI needs to be able to make two requests: (1) the normal search request, and (2) the Flagging request	Both the Flagging Application and the CIR need to be able to connect to all CSs	N/A	When an FP is ADDED, UPDATED or DELETED, the ESB notifies the CIR	N/A	New Flagging Application. The Flagging front-end will handle authorizations, and will use the current CS to query the data. In case the normal (currently already available) request returns a result, the Flagging can be completed by submitting a request to the CIR. If this first search does not return a result, the request is sent to the Flagging Application, which then searches all CSs New CIR. Based on the ESB triggers, the CIR can then UPDATE its identity records that include in which CS the information of the identity is stored
No changes required to component	N/A	N/A		N/A		N/A

4.3 Analysis

The analysis considered 5 distinct criteria against which each of the 5 identified and defined Flagging Options were assessed. The Flagging Options were compared against each other in line with the following criteria:

Criteria	Short Description
Implementation complexity	- Required changes to the ICDs - Migration considerations: Required involvement of MSs and possibility for them to choose moment to implement
Cost/change capacity	- Number of components to change, including expected complexity per component - Complexity of interfaces to change - Required organizational capacity on eu-LISA's side (project management time)
Dependencies	- Impact of major inter-related initiatives on the Flagging Options e.g. ESP, CIR - Alignment with inter-related projects needs e.g. ESP, CIR. Possibility to re-use components - Alignment with architectural principles of an ESB
Legal	Legal clarifications e.g. on data from various CSs residing in the same network zone
IT Security	IT security characteristics, including strengths/ cautions, with a focus on authorization and data separation

The 1-5 scoring scale is easy to understand, yet has proven its efficiency across multiple projects: - - Very low (1), - Low (2), ± Neutral (3), + Good (4), and ++ Very good (5)

4.3.1 Implementation Complexity

Flagging Option	Score	Motivation
Flagging Option 1: Common ESB handles Flagging	--	- All CSs need to be able to authenticate the "Flagging Only" request, send this new request to the ESB, and return the result to the MS. The ICDs between National Access Points (MSs) and the existing CSs (VIS, SISII, EURODAC) need to be changed to accommodate this new functionality - All MSs need to make changes to their National SSIs at the same time to accommodate the new ICDs, as eu-LISA shall not allow the use of multiple ICD versions - Extend the Common ESB with non-ESB tasks to accommodate Flagging requests
Flagging Option 2: Common ESB and Single Instance Shared BMS Handles Flagging	±	- Functionality to query multiple data sets needs to be created e.g. for a VIS Flagging request to search all other data sets of the Single Instance Shared BMS - Queries to the ABIS systems need to be created by the ESB (duplicated functionality, as this is also done in the CSs) - No changes just additions required to the existing CSs ICDs (VIS, SISII, EURODAC) - No changes required to the existing CSs (VIS, SISII, EURODAC) - Small Thin Flagging Application front-end needs to be created
Flagging Option 3: Extra application which handles Flagging	++	- No changes just additions required to the existing CSs ICDs (VIS, SISII, EURODAC) - No changes required to the existing CSs (VIS, SISII, EURODAC) - Small Flagging Application front-end needs to be created to manage authorization and use current CS to query the data
Flagging Option 4: Extra Search and Flagging Orchestrator layer	+	- No changes just additions required to the existing CSs ICDs (VIS, SISII, EURODAC) - No changes required to the existing CSs (VIS, SISII, EURODAC) - The Flagging functionality needs to be integrated in the Search and Flagging Orchestrator - Small Flagging frontend needs to be created
Flagging Option 5: Extra application which handles Flagging with CIR integration	-	- No changes just additions required to the existing CSs ICDs (VIS, SISII, EURODAC) - No changes required to the existing CSs (VIS, SISII, EURODAC) - Small Flagging Application front-end needs to be created to manage authorization and use current CS to query the data - The MSs SSI need to support multiple workflows: (1) the FPs search returns a result, Flagging is completed by submitting a request to CIR, (2) the FPs search does not return a result; then request is sent to Flagging Application, which searches all CSs - Functionality needs to be added to the common ESB: when an FP is ADDED, UPDATED or DELETED, the ESB sends a notification to CIR

4.3.2 Cost/Change Capacity

Flagging Option	Score	Motivation
Flagging Option 1: Common ESB handles Flagging	--	- Change CSs and ICDs = +6x Very Complex Changes; - Change National SSIs (all MSs at the same time) = +25x Very Complex Change - Change Common ESB to include Flagging functionality = 1x Moderately Complex Change
Flagging Option 2: Common ESB and Single Instance Shared BMS Handles Flagging	+	- Create New Thin Flagging Application = 1x Simple Change - Change National SSIs (at MS pace) = +25x Moderately Complex Change - No changes just additions required to existing CSs ICDs = 3x Moderately Complex Change - Change Common ESB to include Flagging functionality = 1x Moderately Complex Change
Flagging Option 3: Extra application which handles Flagging	++	- Create New Flagging Application = 1x Simple Change - Change National SSIs (at MS pace) = +25x Moderately Complex Change
Flagging Option 4: Extra Search and Flagging Orchestrator layer	±	- No changes just additions required to existing CSs ICDs = 3x Moderately Complex Change - Change National SSIs (all MSs at the same time) = +25x Very Complex Change - Flagging functionality to be integrated in Search and Flagging Orchestrator (New component) = 1x Very Complex Change
Flagging Option 5: Extra application which handles Flagging with CIR integration	±	- No changes just additions required to existing CSs ICDs = 3x Moderately Complex Change - Create New Flagging Application = 1x Simple Change - Change National SSIs (all MSs at the same time) = +25x Very Complex Change - Change Common ESB to include Flagging and CIR notifications functionality = 1x Very Complex Change

4.3.3 Dependencies

Flagging Option	Score	Motivation
Flagging Option 1: Common ESB handles Flagging	-	- Prerequisite: The Shared BMS is ready, with either Target State Architecture Option #2 or #3 implemented - All Shared BMS, Target State Architecture Options #2 and #3 from SC82: Common ABIS study Target State Architecture Report are applicable
Flagging Option 2: Common ESB and Single Instance Shared BMS Handles Flagging	--	- Prerequisite: The Shared BMS is ready, and currently retained Target State Architecture Option #3: Common ABIS, separated biometrics databases is implemented - All Shared BMS, Target State Architecture Option #3: Common ABIS, separated biometrics databases considerations from SC82: Common ABIS study Target State Architecture Report are applicable. To consider: high complexity of implementation requiring agreement among all CSs, and higher time to market compared to retained Target State Architecture Option #2: Multiple, highly standardized ABIS images
Flagging Option 3: Extra application which handles Flagging	++	- No major dependencies with any (major) initiative - The implementation of Flagging Option 2 can start right away
Flagging Option 4: Extra Search and Flagging Orchestrator layer	+	Prerequisite: The Flagging functionality is incorporated in the ESP, thus Flagging Option 3 is highly dependent on the ESP implementation
Flagging Option 5: Extra application which handles Flagging with CIR integration	±	Prerequisite: The Flagging Application, as well as the ESB notifications to the CIR are highly dependent on the implementation of the CIR

4.3.4 Legal

Flagging Option	Score	Motivation
Flagging Option 1: Common ESB handles Flagging	±	- The current legal basis for existing CSs (VIS, SISII, EURODAC) prohibit data from being carried over any other network than their own - The additional network zone that connects to all the CSs resides data from all CSs carries queries and consolidated responses. However, only Hit/No hit data elements can be returned
Flagging Option 2: Common ESB and Single Instance Shared BMS Handles Flagging	-	The Shared BMS Target State Architecture Option #3: Common ABIS, separated biometrics databases this Flagging Option is highly dependent on brings about more risks than the other retained option, mainly from a data protection (integrity and confidentiality) perspective, as well as the requirement to update/ change existing regulations for each CS within the Shared BMS to meet the needs to regulate e.g. how data privacy will be guaranteed needs to be addressed (e.g. tagging, multi-layer access control, encryption)
Flagging Option 3: Extra application which handles Flagging	±	- The current legal basis for existing CSs (VIS, SISII, EURODAC) prohibit data from being carried over any other network than their own - The additional network zone that connects to all the CSs resides data from all CSs carries queries and consolidated responses. However, only Hit/No hit data elements can be returned
Flagging Option 4: Extra Search and Flagging Orchestrator layer	±	- The current legal basis for existing CSs (VIS, SISII, EURODAC) prohibit data from being carried over any other network than their own - The additional network zone that connects to all the CSs resides data from all CSs carries queries and consolidated responses. However, only Hit/No hit data elements can be returned
Flagging Option 5: Extra application which handles Flagging with CIR integration	-	- The current legal basis for existing CSs (VIS, SISII, EURODAC) prohibit data from being carried over any other network than their own - The additional network zone that connects to all the CSs resides data from all CSs carries queries and consolidated responses. However, only Hit/No hit data elements can be returned

4.3.5 IT Security

	Score	Motivation
Flagging Option 1: Common ESB handles Flagging	++	- No additional point of exposure is created - Authorization is managed in the CSs and in the common ESB - One new role needs to be created per MS to give the End-User access to the Flagging functionality - The Flagging functionality uses the same authorization mechanisms as currently in use by the CSs
Flagging Option 2: Common ESB and Single Instance Shared BMS Handles Flagging	--	- One additional point of exposure is created by adding the Thin Flagging Application, which also handles authorization - All Shared BMS, Target State Architecture Option #3: Common ABIS, separated biometrics databases considerations from SC82: Common ABIS study Target State Architecture Report are applicable. To consider: IT Security of the ABIS system's "black box" needs to be trusted, with currently limited built-in application security; since all data resides on the same virtual network, one IT security or configuration issue could be sufficient to breach from e.g. SISII to EURODAC data, difficulty to monitor such breaches as it is not possible to rely on VM or network logging to detect breaches etc - Target State Architecture Option #3: Common ABIS, separated biometrics databases exudes the most IT Security and Compliance risks compared to the other Target State Architecture Options - One new role needs to be created per MS to give the End-User access to the Flagging functionality - The Flagging functionality uses the same authorization mechanisms as currently in use by the CSs
Flagging Option 3: Extra application which handles Flagging	±	- One additional point of exposure is created by adding the Thin Flagging Application, which also handles authorization - One new role needs to be created per MS to give the End-User access to the Flagging functionality - The Flagging functionality uses the same authorization mechanisms as currently in use by the CSs
Flagging Option 4: Extra Search and Flagging Orchestrator layer	-	- One additional point of exposure is created by adding the Extra Search and Flagging Orchestrator layer - Different IT Security levels should be in place in the Extra Search and Flagging Orchestrator layer in line with the CS or network used to access the Extra Search and Flagging Orchestrator layer - Authorization is handled in the Flagging Application encapsulated in the Extra Search and Flagging Orchestrator layer - One new role needs to be created per MS to give the End-User access to the Flagging functionality - The Flagging functionality uses the same authorization mechanisms as currently in use by the CSs
Flagging Option 5: Extra application which handles Flagging with CIR integration	±	- One additional point of exposure is created by adding the Thin Flagging Application, which also handles authorization - One new role needs to be created per MS to give the End-User access to the Flagging functionality - The Flagging functionality uses the same authorization mechanisms as currently in use by the CSs

4.3.6 Summary of Comparison Results

Criteria	Flagging Option 1: Common ESB handles Flagging	Flagging Option 2: Common ESB and Single Instance Shared BMS Handles Flagging	Flagging Option 3: Extra application which handles Flagging	Flagging Option 4: Extra Search and Flagging Orchestrator layer	Flagging Option 5: Extra application which handles Flagging with CIR integration
5.1 Implementation complexity	--	±	++	+	-
5.2 Cost/change capacity	--	+	++	±	±
5.3 Dependencies	-	--	++	+	±
5.4 Legal	±	-	±	±	-
5.5 IT Security	++	--	±	-	±
Fittest Flagging Options			Fittest Flagging Option	Fittest Flagging Option considering the entire architecture	
Possible with Shared BMS Target State Architecture Options*	2, 3, 4, 5, 6	3, 5	All	All	2, 3, 4, 5, 6,
Potential Timeline	36 months	72 months	24 months	48 months	48 months

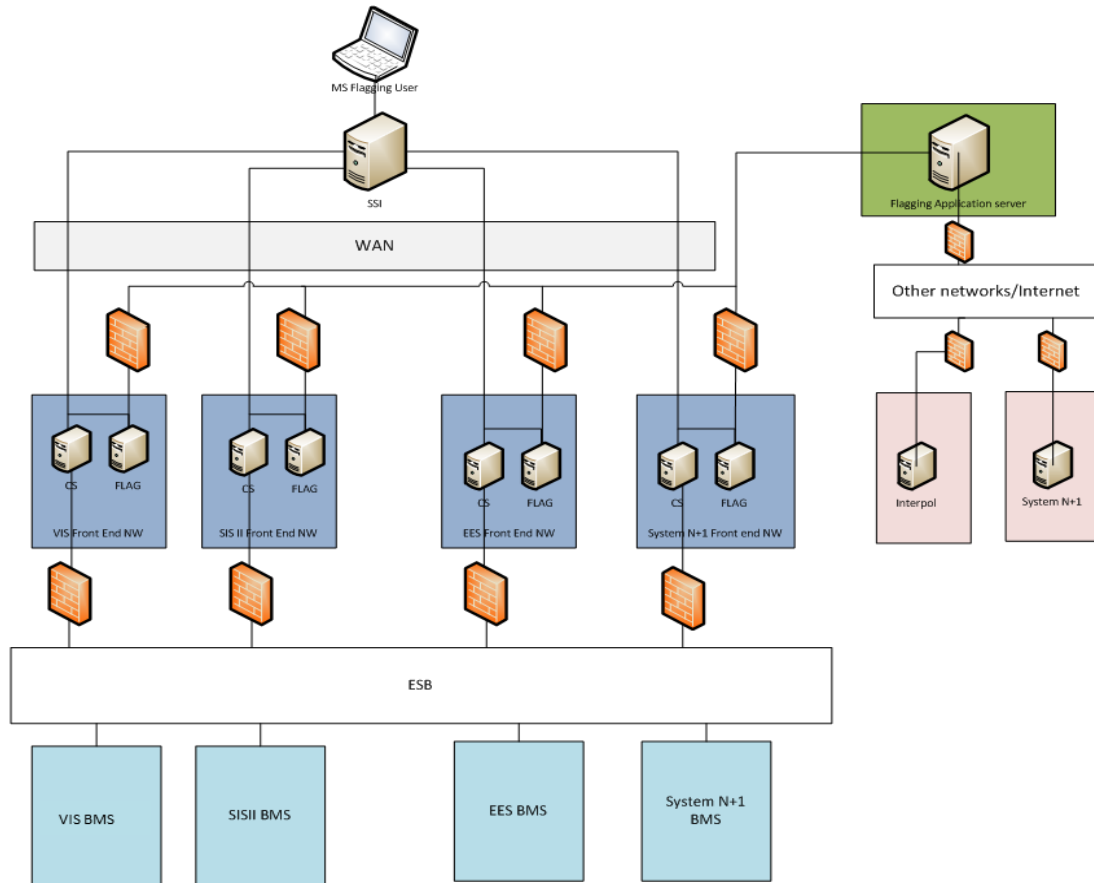
4.3.7 Further considerations for Fittest Flagging Options

For the two Fittest Flagging Options, which from an architectural perspective are similar, the following components are detailed further:

- High-level Network Overview
- Flagging Workflow, including NIST translation considerations
- Silent Notification and SIRENE Messages Workflow
- Proposed Flagging Message Design
- Recommended technologies for the Flagging gateway and the Flagging Application

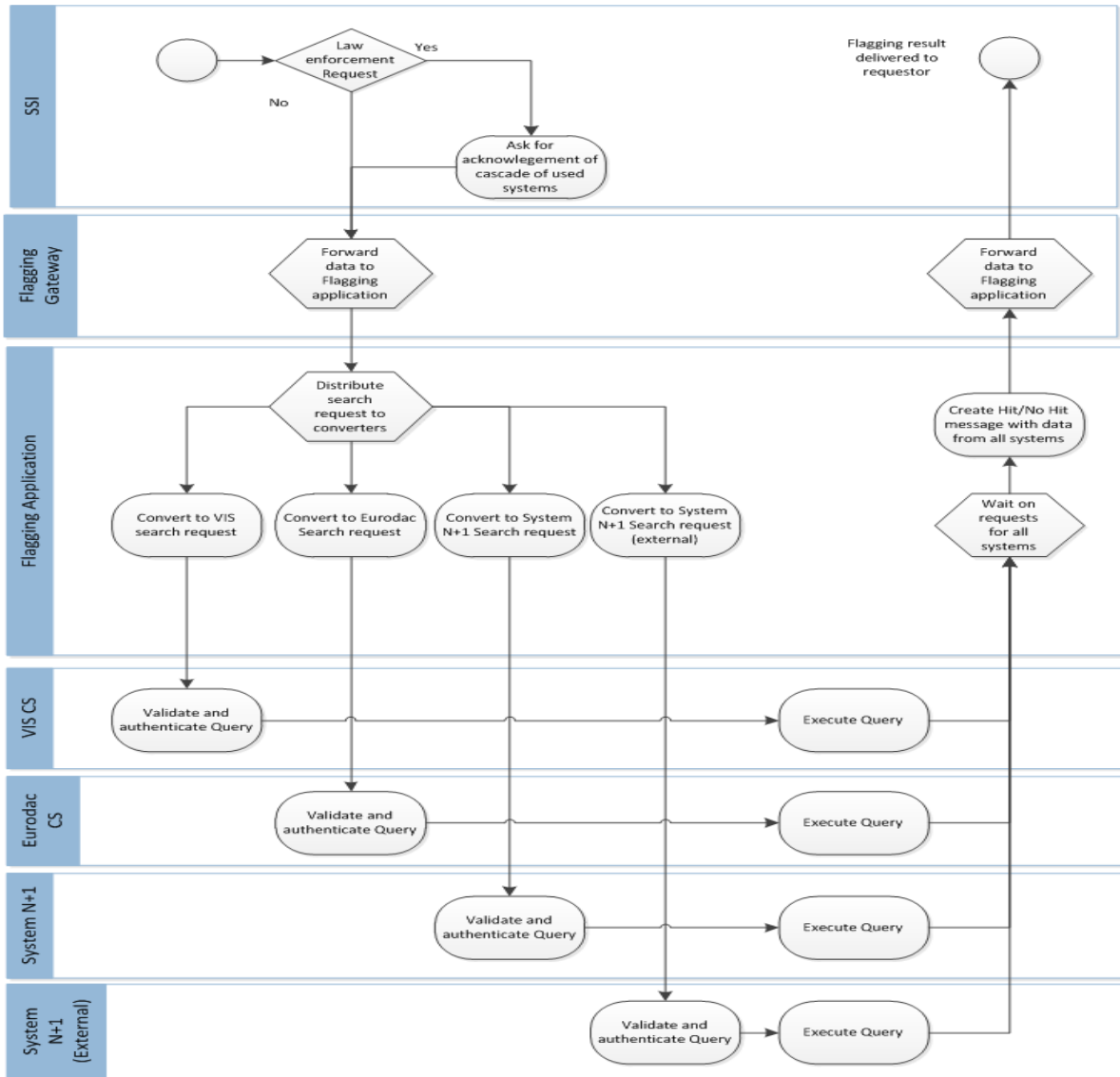
4.3.7.1. High Level Network Overview

- The Flagging functionality of the National SSI would connect to the Flagging gateway server in the network it already has access to.
- This Flagging gateway server would act as a communication channel to the Flagging Application server, ensuring proper separation of networks.
- The Flagging Application server would also be connected to other networks/Internet e.g. Interpol, Europol.
- The Flagging gateway servers would not connect to the ABIS systems e.g. EES BMS, SIS II BMS, VIS BMS.



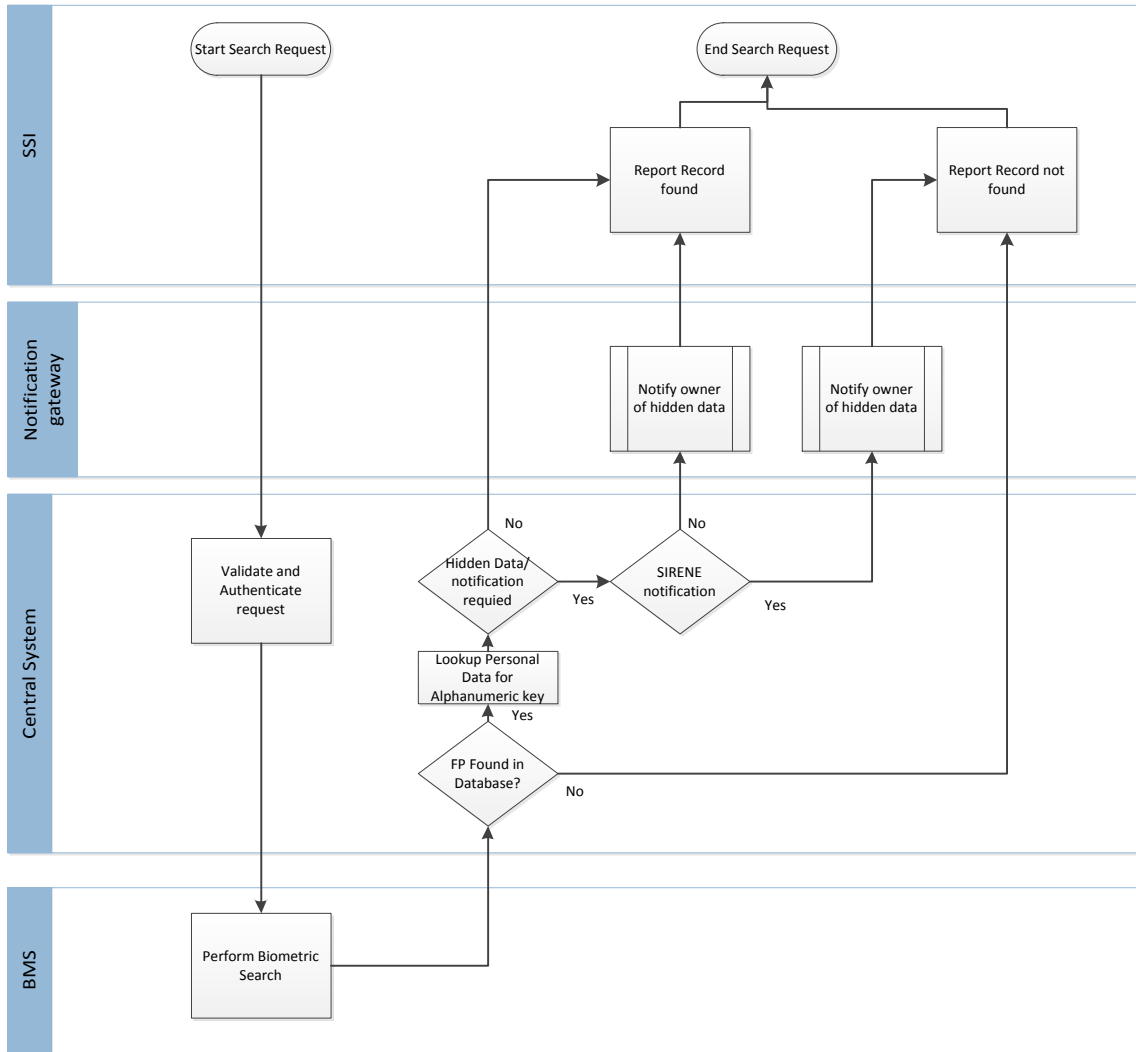
4.3.7.2. Flagging Workflow, including NIST translation considerations

- If an MS wants to use the Flagging functionality, it would need to change their National SSI to make Flagging visible or may use a dedicated User to System Interface (Web GUI, potentially provided by eu-LISA) if it does not require changes to their National SSI
- The updated module could send the same message format used for Search to the Flagging Application. This would make the implementation easier
- The Flagging Application could use the already existing ICDs to query the CSs. ABIS vendors confirmed it is possible to convert all search requests containing a NIST file so that it can be used to query the other existing CSs
- The only new message would be the retrieved message and would contain the Hit/No hit data elements
- The Flagging Gateway could be used for IT Security purposes (please consult the 'High-level Network Overview' for more details), and would be transparent to the End-Users



4.3.7.3. Silent Notification and SIRENE Messages Workflow

- The biometrics Search response from CSs could be required to be hidden from the Search issuer in the MS due to applicable restrictions on the data e.g. the search request is sent over the VIS network, thus SIS responses need to be hidden
- Hidden search responses could be configured to trigger SIRENE notifications in the respective CS, independent of the Search response sent to the National SSI and the end-user in the MS
- The Silent Notification and hiding of certain records has no dependencies with Flagging as both normal searches and Flagging searches need to notify the data owners
- The Silent Notification could be performed by sending an encrypted and secure email to the data owner(s)



4.3.7.4. Proposed Flagging Message Design

- According to the proposed setup, no changes are required to the existing ICDs. If a VIS user wants to perform a Flagging request, the same message can be sent to the Flagging Gateway
- The only new message would be the response message reporting back to the end-user in the relevant MS
- In order to minimize the required changes to the National SSIs, it is recommended to re-use the current technologies in place

5. Conclusions and Recommendations

General conclusions of the Architectural Options:

The overall ranking score of Option #1 – an optimised version of the current setup - clearly indicates that it is unsuitable for future considerations. Thus, development of some form of shared BMS is recommended.

Based on the comparison and ranking exercise across the 8 criteria, eu-LISA has identified that Option #6", named "common Shared Biometric Services Platform" (cSBSP) is the fittest architectural option. The cSBSP makes use of all identified advantages of the other considered options and minimises identified disadvantages to the best extent possible. Options #3 and #4 would be the next preferred options.

Option #2 and Option #4 provide for better operational business continuity than is currently possible but introduce only partially the needed technical flexibility for the required strategic business continuity. Options #3 and #5 provide for improved technical flexibility and strategic business continuity but only partially address needs for operational business continuity.

Recommendations for the Target Architecture:

After the overall assessment of the study, eu-LISA would like to express the following recommendations:

- Design and implement a "common Shared Biometric Service Platform" (cSBSP), as previously described at high level
- Make sure the resulting System is suitably modularized, namely using layers to segregate the Business Systems from the matching engines, thereby ensuring the least amount of inter-service impact in the case of changes and at the same time reaching the maximum in flexibility and business continuity advantages (operational and strategic)
- Introduce the possibility for "soft migration" for the future to come in case of adjusting matching engines by changing technology or vendor
- Ensure a future-proof solution by choosing a solid enterprise-infrastructure-platform as the foundation to build on and make use of state of the art technologies for large IT operations
- Take into account the use of state of the art Data Centre technologies to ensure less cost-intensive operations in terms of currency and HR
- Take into account an Active-Active-by design architecture to ensure business continuity for the critical systems at eu-LISA
- Strategically prevent future vendor-lock-in by investing in a highly flexible design, capable of well planned and executed migration across evolving technologies within potential product-life-cycle time periods (3-5 years)
- Strategically invest in a system designed to be able to react quickly to potential discontinuation of current technologies without the threat of disrupting vital security IT-Systems

General conclusions of the Migration Options:

According to the impact assessment results across the 5 criteria, both assessed options have pros and cons and neither option stands out immediately as more optimal. Thus, further discussion would be required to select the migration approach towards migration to a future sBMS. This would, by necessity, involve Member States and

their end users and have to take into account the business needs of the systems, the readiness of the MS to make changes of their own necessary at points in time, on-going activities at eu-LISA and MS level and the speed with which the sBMS functionality would need to be incorporated into each application.

Recommendations for the Migration Options:

Ensure buy in for a more standardized way of working. The implementation and roll-out will lead to many changes in both the systems and the way the systems are operated due to standardization. Furthermore, future changes will possibly be more complex due to a higher degree of standardization.

Investigate with legal experts to which extent the legal bases have to change. Although the legal base is not specific on configuration or security setup, it is recommended to investigate this with legal experts to avoid issues later.

Expect significant testing if there is more significant changes in architecture or technologies deployed. Most Member States are familiar with the current ABIS provider. Although a new vendor could provide a similar level of accuracy, Member states might want to perform more extensive testing in order to prove this point in the eu-LISA context.

Create and formalize a Common ABIS system dedicated test document complementing eu-LISA's existing Test Strategy (Dec, 2016) describing in more detail how to test the new systems on security, performance, availability and accuracy. This will increase the level of trust in the new systems and migration plan.

Ensure the System Integrator(s) (implementer(s)) has/have a proven track record. There are few 100M+ ABIS implementations in the world, so choosing a vendor with a proven track record in large ABIS implementations with the ability to deploy local experts is a key driver in the success of the ABIS implementation.

General conclusions of the Flagging Functionality Assessment

The Flagging option with the highest fitness is the option where an extra application handles the Flagging (Flagging Option 3); however, in case the ESP is implemented, from an architectural perspective, the Flagging functionality could be integrated in the ESP. While the Shared BMS is needed to implement Flagging Options 1, 2 and 5, Flagging Options 3 and 4 can be implemented irrespective of the existence of a sBMS.



© European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, 2018

ISBN 978-92-95208-73-5

doi:10.2857/84504