Elaboration of a Future Architecture for Interoperable IT Systems at eu-LISA

Summary of the Feasibility Study

2019

To contact eu-LISA for further information, please email research@eulisa.europa.eu.
For enquiries regarding further use of this paper or the information contained herein, please contact communications@eulisa.europa.eu.

ISBN 978-92-95217-53-9
doi:10.2857/020572
Catalogue number: EL-04-19-542-EN-N

Contents

Introduction 4
Background 4
Objective and structure of the Feasibility Study 5
Deliverables 6
Architecture Principles 6
Suggested Architecture Options 8
Key symbols in visualisation 8
Implementation of the architecture options 9
Implementation timeline 10
Impact Assessment and Planning 11
Impact on Core Business Systems (CBS) 11
IT Security, Compliance and Privacy by Design 11
Findings and conclusions 13
Conclusions and implementations success factors 13

Introduction

This paper introduces the main goals, deliverables and conclusions of the feasibility study 'Elaboration of a future architectural framework for interoperable IT systems at eu-LISA: impact assessment and migration and integration plan'.

The work on the study started in September 2018 and was completed in June 2019.

The aims of the study were to identify and analyse the feasibility of various options for the architectural design and development of future systems by the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), along with the interoperability components (as described in the interoperability regulations), and thus to assess the architectural possibilities for deploying the solutions and to outline perceived optimal architectural descriptions in the form of architectural description artefacts.

Background

In recent years, the areas of border management, internal security and migration management have been going through a major transformation, moving from the physical to the virtual world. Fragmentation among the existing EU information systems makes data access complex. This can lead to blind spots for law enforcement and other authorities, as it can be very difficult to recognise connections between data sets. Interoperability across the various information systems at EU level seeks to address this fragmentation. Through interoperability, systems will be able to supplement each other so that the appropriate authorities have access to the information they need, when they need it. Thus, interoperability between systems will help in tackling irregular migration, correctly identifying persons, fighting identity fraud and validating travel documents, and will ultimately contribute to a higher level of security in the area of freedom, security and justice in the EU.

The general objectives of the regulations on interoperability of systems and components (Regulation (EU) 2019/817 ([1]) on borders and visa and Regulation (EU) 2019/818 ([2]) on police and judicial cooperation, asylum and migration) are improving the management of the Schengen external borders and contributing to the internal security of the EU. They stem from policy decisions by the European Commission and relevant European Council conclusions. These objectives were also set out in the European Agenda on Migration and subsequent communications, including the communication on preserving and strengthening Schengen ([3]), the European Agenda on Security ([4]) and the Commission's work and progress reports on an effective and genuine Security Union ([5]).

The regulations were adopted in May 2019 and entered into force in June 2019. The regulations provide for the development of the following interoperability components: the European Search Portal (ESP), the

([1]) Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135, 22.5.2019, p. 27-84 (available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0817).
([2]) Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135, 22.5.2019, p. 85-135 (available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0818).
([3]) Communication from the Commission to the European Parliament and the Council on preserving and strengthening Schengen, Brussels, 27.9.2017 (COM(2017) 570 final).
([4]) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions — The European Agenda on Security, Strasbourg, 28.4.2015 (COM(2015) 185 final).
([5]) Communication from the Commission to the European Parliament, the European Council and the Council — Delivering on the European Agenda on Security to fight against terrorism and pave the way towards and effective and genuine Security Union, Brussels, 20.4.2016 (COM(2016) 230 final).

shared Biometric Matching Service (sBMS), the Common Identity Repository (CIR), the Multiple Identity Detector (MID) and the Central Repository for Reporting and Statistics (CRRS). The components are to cover the systems that are already operational (the second generation Schengen Information System (SIS II), the Visa Information System (VIS) and the European Asylum Dactyloscopy Database (Eurodac)) as well as three new systems that are in planning and development (the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS) and the European Criminal Records Information System for Third Country Nationals (ECRIS-TCN)).

Building in particular on the April 2016 Commission communication 'Stronger and smarter information systems for borders and security' and the final report of the High-Level Expert Group on Interoperability, the specific objective of these regulations is to ensure that end-users have fast, seamless, systematic and controlled access to the information stored in the systems, providing solutions for detecting multiple identities linked to the same set of biometric data with the purpose of ensuring the correct identification of persons, thus combating identity fraud. Furthermore, the implementation of these components will facilitate identity checks on third country nationals on the territory of a Member State by the relevant authorities and streamline access by law enforcement authorities to non-law enforcement information systems at EU level for the prevention, detection or prosecution of serious crime and terrorism.

Given the significant changes to come, it is critical that new developments and evolutions currently being planned and even under way proceed with full knowledge of the intended future state. This is particularly true for EES and ETIAS, development of which will begin very soon; the EES will be the first eu-LISA system to be built in an interoperable environment, incorporating not only a secure communication channel with VIS but also biometric systems that will be the basis for the sBMS.

Objective and structure of the feasibility study

The objective of the study was to map out the desired future interoperability architecture — which includes the interoperability components mentioned above and the existing and future systems managed by eu-LISA — from both enterprise and technical/informational architecture perspectives. This is considered a vital contribution to work on the evolution of current systems and the development of new systems as well as to the development of the interoperability components themselves. Furthermore, an impact assessment (covering security/data protection, financial resources, human resources, procurement, technology, etc.), including a complete picture of the interfaces between the interoperability components and the existing and new systems together with an outline plan for migration to the new interoperability architecture, was also part of this work.

The study was split into three work packages (WPs):

- WP1 — elaboration of a future architectural framework for interoperable IT systems at eu-LISA;
- WP2 — implementation of service-oriented architecture (SOA) (including the use of an enterprise service bus (ESB));
- WP3 — impact assessment and migration and integration plan towards the future interoperable architecture.

The first WP focused on proposing three possible interoperability architectural options, from which a preferred one was selected; an architecture development cycle was then developed to the appropriate extent. The recommendations emphasised the architectural interfaces and implementation possibilities for all interoperability components, starting with their functional features and technical functionalities, and continuing through all interoperability interfaces and the integration of existing and new systems.

The second WP concentrated on the feasibility and benefits of implementing SOA (including, if appropriate, the use of an ESB and application programming interfaces (APIs)).

The third WP took the outcomes of WP1 and WP2 forward and focused on the main impacts of the future architectural options outlined on the organisation and operational model of the Agency. A high-level migration and integration plan was created, detailing how the transition between the present and the new architecture might be done, mitigating negative impacts and maximising positive impacts in the coming years.

Deliverables

The following deliverables were produced within the scope of the study:

- an architecture vision document, which presents a high-level aspirational view of the final architecture product;
- an architecture requirements specification, which defines the high-level requirements for the target architecture;
- an architecture definition document, which describes the target architecture in relation to the business, applications, data, technology and security domains;
- architecture building blocks, which specify the various application architecture building blocks for the interoperability components;
- an architecture repository, which consists of a structural framework enabling eu-LISA to differentiate between different types of architectural assets;
- an SOA reference architecture, which explores the capabilities and benefits of adopting integration, SOA and API-based solutions;
- recommended usage patterns and guidelines for SOA, which present guidelines and recommendations on when SOA should be introduced;
- an SOA runtime architecture, which sets out considerations on runtime management and monitoring and organisational management in SOA;
- a requirements impact assessment, which analyses the new requirements and their impacts on organisational and architectural levels;
- an architecture roadmap, which summarises the initiatives to be undertaken to transition from the baseline architecture to the target architecture.

Architecture principles

The architectural principles listed in the table below were taken into account when designing the options.

#ID	*Principle*	*Description*
P1	**Primacy of principles**	The principles defined apply to the entire architecture work of the core business systems (CBS) life cycle
P2	**Full compliance with legal instruments**	The Agency is to abide by the relevant legal instruments
P3	**Maximise benefit to the Agency**	Information management decisions are made to provide maximum benefit to the Agency as a whole
P4	**Business continuity**	System operations shall be maintained and data persistence assured by having regard for the following design features: resilience, availability and recoverability

#ID	Principle	Description
P5	**European interoperability approach**	Software and hardware should conform to clearly defined standards that promote interoperability for data, applications and technology
P6	**Common vocabulary and data definitions**	Data is defined consistently throughout the CBS, and the definitions are understandable and available to all stakeholders
P7	**Data is an asset and its quality must be ensured**	Data is understood to be a valuable resource and has real, measurable value for the Agency
P8	**Data has a single authoritative source**	Each data element has a single authoritative source that ensures the integrity of the data. This authoritative source is generally identified based on the business process that initially captured the data
P9	**Service orientation**	An application must be composed of different services, each loosely coupled to the others, independent and adhering to a bounded context
P10	**Continuous integration**	Building and testing are automated processes enabling continuous quality control
P11	**Use of multiple application platform environments**	Different application platform environments exist within the Agency (production, preproduction, 'other')
P12	**Monitoring and measurement**	Large-scale IT systems will be designed to support monitoring and measurement
P13	**Technology independent of applications**	Applications are independent of specific middleware technology choices
P14	**Scalability by design**	The technology platform and applications should be able to be scaled up by adding more instances, ideally in a linear way
P15	**Control technical diversity**	Controlling technical diversity reduces the non-trivial cost of human resources and expertise
P16	**Build securely by design**	Every system managed by eu-LISA must guarantee the fulfilment of the following security requirements: confidentiality, integrity, availability, accountability and non-repudiation
P17	**Maintain, adapt and evolve security posture**	Any set of security requirements must be able to adapt and evolve to deal with new and emerging risks, technologies, threats, and legal and organisational contexts
P18	**Privacy by design**	The CBS processes must be designed from the start to adhere to data protection principles so that only personal data that is necessary for a specific purpose is processed. This applies to the amount of personal data collected, the extent of its processing, the period of its storage and its accessibility (in accordance with the General Data Protection Regulation)

Suggested architecture options

Three architecture options were developed, as shown in Figure 1. (limited here to a conceptual representation):

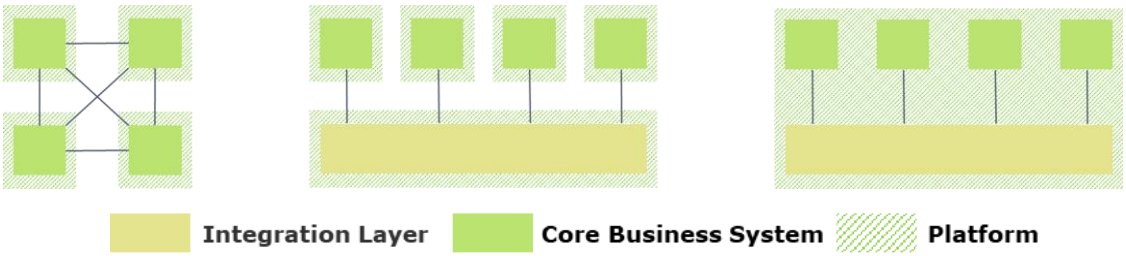

Figure 1. *The three architecture options: Continuation (left), Integration (middle) and Unification (right)*

The first architecture option, Continuation, is based on the point-to-point principle. In such an architecture, new systems are connected directly with each other, without any form of middleware. Thus, the systems communicate directly with one another, retaining all logic internally. This method of working is the current way in which systems are connected in the eu-LISA landscape. If the interoperability components were introduced using the Continuation option, the number of internal connections required would be 33.

The second architecture option, Integration, introduces the concept of an integration layer. This integration layer acts as an orchestration layer connecting the various CBS. In practice, systems are connected to, and communicate with, the integration layer only. This implies that, when introducing a new system to the architecture, only a single new connection would be required. If the eu-LISA landscape transformation were implemented using the Integration option, the number of internal connections required would fall to 11.

The third architecture option, Unification, retains the integration layer as described in Integration. This option differs on the platform level. Instead of each component and CBS operating on its own dedicated platform, Unification proposes a common interoperable platform on which all components and CBS would operate. This option leverages eu-LISA's common shared infrastructure (CSI) as the basis of the common interoperable platform.

Key symbols used in visualisation

The options were visualised using the symbols and colour codes shown in Figure 2.

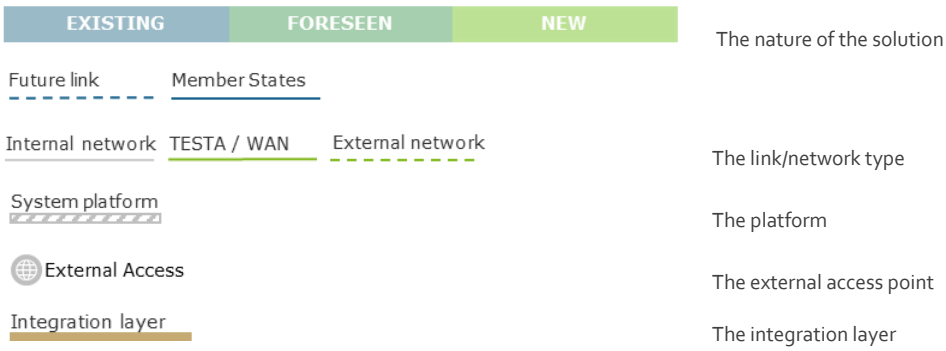

Figure 2. *The symbols and colour codes used in the architecture plans*

Implementation of the architecture options

Conceptual models of the Integration and Unification options are presented in Figures 3 and 4 respectively.

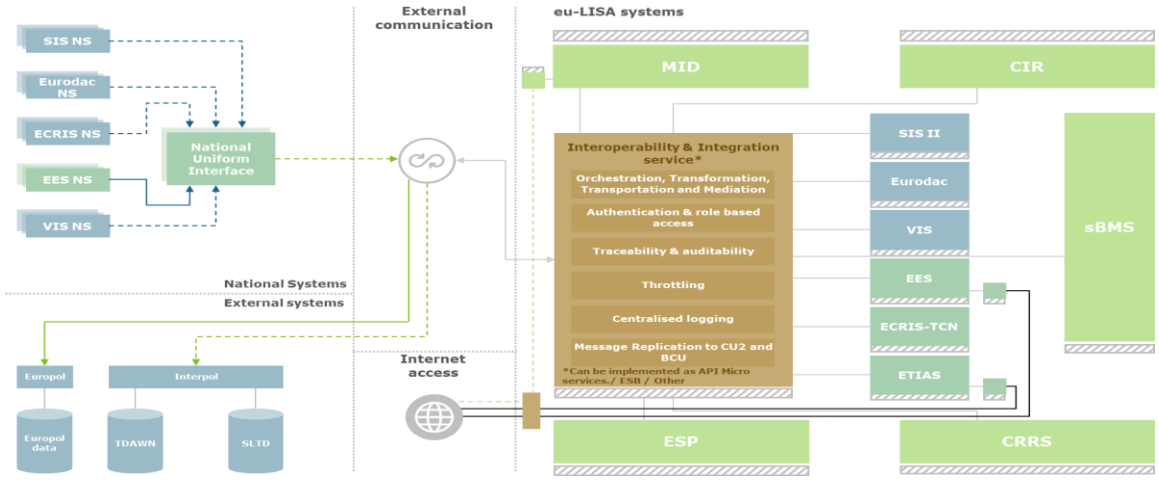

Figure 3. *Conceptual model of the Integration option*

The integration layer simplifies communication, governance and system integration. Introducing this layer to the architecture would further centralise system-to-system communication, orchestration and information flows, all of which are currently distributed across different applications and legacy systems in the eu-LISA landscape. This does not preclude that mechanisms such as security or logging should be disregarded in each system, and completely moved to this new integration layer.

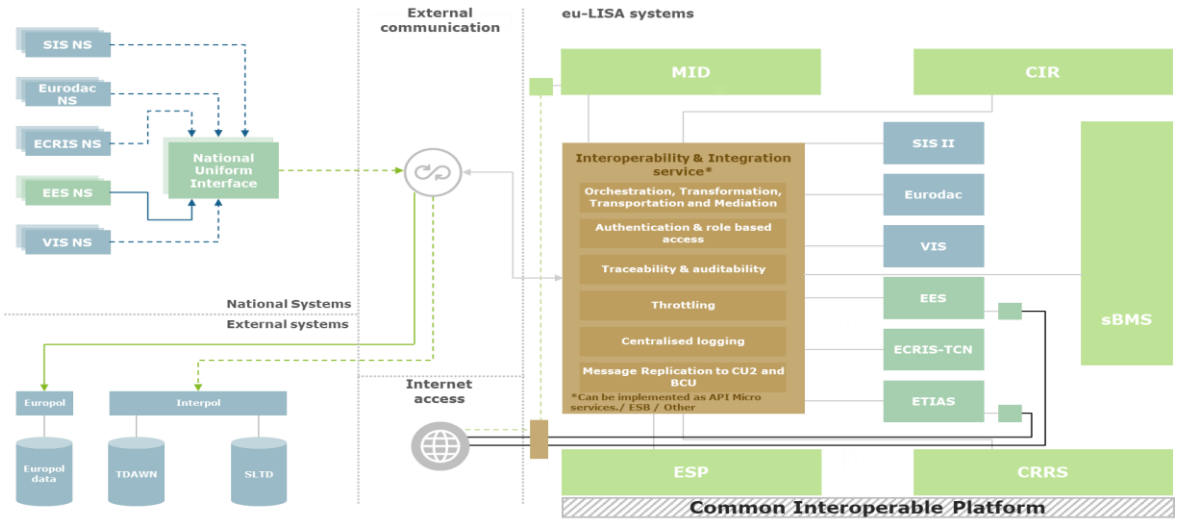

Figure 4. *Conceptual model of the Unification option*

Unification differs in that it adopts a common interoperable platform. Instead of each component and system operating on its own dedicated platform, they would all share this common interoperable platform. This would be in line with the current plans for the evolution of the CSI.

Implementation timeline

The implementation and migration plan included in the study is entirely based on the latest indicative timeline provided by the European Commission (Figure 5).

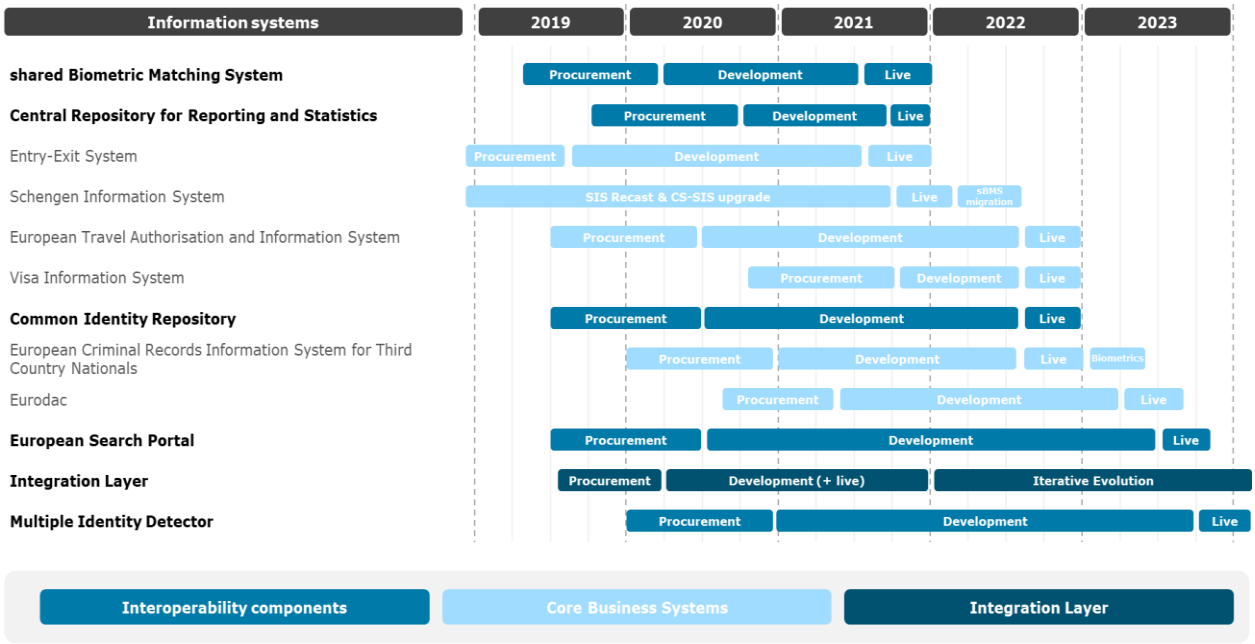

Figure 5. *Implementation plan roadmap*

Aside from implementation, there are also migration efforts to be considered (Figure 6). The recommendation is that these happen prior to the go-live of the various systems, the key reason being that if this were not the case there would first have to be a migration from the legacy CBS to the recast versions.

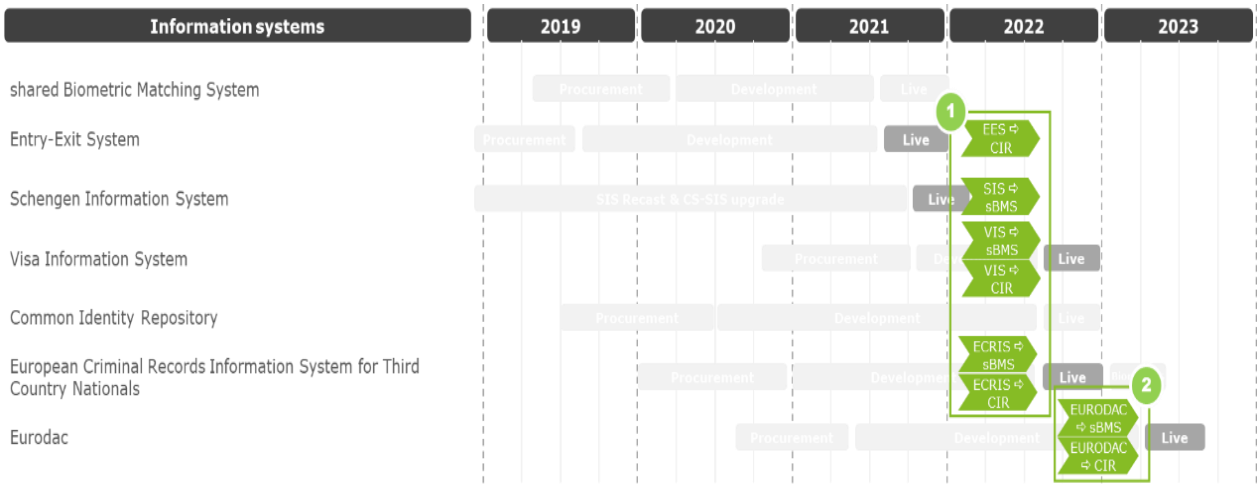

Figure 6. *Migration plan roadmap*

Impact assessment and planning

In the final phases of the project, a more detailed impact assessment on certain aspects was carried out. In addition, an initial implementation and migration plan was developed.

The following topics were considered in this respect:

- core business systems
- impact on business organisation
- IT security, compliance and privacy by design
- technology and infrastructure
- cost analysis
- mapping to the new eu-LISA procurement model.

Impact on core business systems

Each CBS will need to implement a connector to the integration layer to allow communication and data exchange with other CBS and the interoperability components.

The introduction of the CIR will require CBS to migrate their identity, travel document and raw biometric data.

The introduction of the sBMS will require modifications to CBS.

The introduction of the CRRS will require CBS to change how they handle reporting and statistical data. Instead of handling these tasks internally, the CBS will push the relevant data to the CRRS.

IT security, compliance and privacy by design

An impact assessment has been conducted on the architecture's security domains, data security/protection, security functions, operational security, maintainability, changeability and compliance with legal bases.

The following assessments have been made per category:

- The integration layer offers central oversight of security controls and their implementation and evolutionary capabilities for data security. Therefore, there will be a positive impact.
- The integration layer orchestrates and supports multiple security functions. Due to the centralised nature of the integration layer, certain security functions thus no longer need to be duplicated in each system. Therefore, there will be a positive impact.
- The security of the systems is no longer the responsibility of individual system owners. The orchestration layer requires monitoring controls during operation, which leads to shared responsibilities among system owners. Because the integration layer effectively integrates all the systems in the landscape, the currently limited operational security is improved by this centralisation of responsibilities. Therefore, there will be a positive impact.
- The integration layer introduces an extra component that needs to be maintained. However, as CBS and interoperability components only need to connect to the integration layer, the number of connections between systems will increase linearly according to the number of connected systems. This leads to an architecture that is overall easier to maintain. Therefore, there will be a positive impact.
- In the current architecture, because systems are not interoperable, they may evolve independently from one another, which eventually leads to a divergence across the architecture landscape. When

this happens, the changeability of the architecture is at an absolute minimum. The integration layer will constrain the divergence of the individual systems, facilitating an iterative approach to change. Therefore, there will be a positive impact.

Findings and conclusions

An impact assessment on the three architecture options was made taking into account a set of 11 criteria (IT security, compliance and privacy by design; impact on legal basis; integration and interconnectivity; flexibility; technology independence of applications; scalability by design, capacity and performance; business continuity; complexity of implementation; time to market; implementation and operational cost; and implications for procurement).

Based on the results, the recommendation was made that Integration could be selected as the current preferred target architecture. Eventually, there will be a transformation to Unification; however, the effort required to introduce the common interoperable platform, on top of all the other ongoing initiatives, is deemed not feasible at this time and will need to be undertaken gradually. The analysis also resulted in a recommendation that eu-LISA opt for SOA with API-led connectivity.

An additional impact assessment was performed on eu-LISA's target architecture, and the following topics were considered: core business systems; impact on business organisation; IT security, compliance and privacy by design; technology and infrastructure; cost analysis; and mapping to the new eu-LISA procurement model.

Conclusions and implementation success factors

The study resulted in a list of the five most critical success factors for the successful completion of the upcoming initiatives (as shown in Figure 7 and listed below). These success factors relate mostly to the organisational level, as interoperability between systems is a new concept that will require engagement from the entire Agency.

Figure 7. *Key success factors — interoperability and transversal working*

(1) **The establishment of an effective and decisive design authority.** The authority should take the architectural and design decisions that affect the Agency and one or more supplier(s), so as to achieve consistency and alignment between suppliers and the Agency, and between different suppliers, such that everything fits together and meets the required standards.

(2) **The transformation of the CSI into a common platform.** Over time, the CSI should be made into the proposed common interoperable platform. This will lead to assets fitting the procurement roadmap (top down) as opposed to technologies being spun up (bottom up).

(3) **Following the principle of 'buy over build'.** This means that commercial off-the-shelf (COTS) products should be favoured wherever possible. Systems should be custom built only where a COTS solution is not available.

(4) **Permission to operate at scale and pace.** The upcoming initiatives are unlike any other the Agency has implemented so far. Multiple procurements will be happening simultaneously, involving multiple vendors. These vendors will also need to cooperate closely in order for the systems to work together seamlessly. A strict governance strategy across multiple lots will be needed to ensure that the Agency can operate on a larger scale and deliver in a timely manner.

(5) **Permission to drive change in the Agency.** The total transformation of the architecture will induce change on many levels. This change needs to be accepted by all stakeholders. Note that this factor is closely linked to success factor 4. For this shift in mentality to happen, new behaviours, tools and processes must be encouraged and promoted.

The evolution of the current systems, the development of the new systems and the introduction of interoperability of information systems will foster cooperation in the area of justice and home affairs and reinforce the EU's internal security.

The results of the study give a 360-degree holistic view of what the options for the implementation of the new systems are and what is needed in terms of interfaces and high-level updates to the existing systems. Therefore, the architecture roadmap, definition and building blocks created as part of this study will be further developed and used as a solid basis for all future initiatives in this regard.

EL-04-19-542-EN-N

ISBN: 978-92-95217-53-9
doi: 10.2857/020572