MANAGEMENT OF THE REFERENCE ARCHITECTURE OF EUROPEAN INFORMATION SYSTEMS AND INTEROPERABILITY COMPONENTS IMPLEMENTED IN THE SECURITY INFRASTRUCTURE

Petrică TERTEREANU[1]
Alexandra Ioana GÎNGU[2]
Aurel Mihail ŢÎŢU[3,4,5]

***Abstract*:** *The scientific paper addresses a topical issue regarding the management of the European information systems architecture and interoperability constituents applied in the security infrastructure. The authors set out to provide their own views on the technical framework for the operationalization and implementation of the interoperability framework for existing and developing European information systems at national level. Scientific research highlights the process of implementing the new architecture of European information systems that aims to develop and implement interoperability components. At present, the concept of interoperability at European level addressed in the context of cross-border cooperation does not have common infrastructures and technical guidelines, which should provide a solid technical basis. The implementation of the interoperability framework at the level of European information systems can be a first step in raising awareness of this issue, in the sense of addressing the concept of interoperability at the level of digital public services. All the above presented their explanations in the present scientific paper and the authors propose a personalized and reasoned point of view related to those mentioned*

Keywords: information system, quality and security, security systems technology, interoperability.
Jel Classification: O10, O20

[1] County Police Inspectorate Valcea, Vâlcea, Romania, tertereanupetrica@yahoo.com
[2] Thetys Pumps Company, Bucharest, Romania, alexandra.gingu@yahoo.com
[3] Lucian Blaga University of Sibiu, Sibiu, Romania, mihail.titu@ulbsibiu.ro
[4] The Academy of Romanian Scientists, Bucharest, Romania, mihail.titu@ulbsibiu.ro
[5] Romanian Association for Alternative Technologies Sibiu, Sibiu, Romania, mihail.titu@ ulbsibiu.ro

1. Introduction

"The European Union has built a number of databases. But often these databases do not talk to each other."

The Commission is trying to change this by doing two things: first, it wants border guards and law enforcement to be able to get all the information they need about a person with a single-click. The European Union was hit by a double migration crisis and a series of terrorist attacks in 2015 and 2016, which revealed shortcomings in the bloc's security agreements and created friction between Member States. In response, the EU has promised to make the safety of its citizens a major concern. In 2016, the European Commission launched the Security Union. Commissioner Schinas described the Security Union as a new single-roofed house, in which the EU seeks to build a new security ecosystem that covers the full spectrum of policies.

In general, SUS seeks to facilitate the development of capabilities and capacities to strengthen the EU's resilience to the threats and challenges it faces. The Security Union aims to close the gaps in EU's security coordination, focusing on five main areas: data collection and exchange; border controls; terrorism and organized crime; cyber security; cooperation with third countries. In the context of efforts to combat terrorist attacks, the EU is improving its ability to apprehend criminals and suspects and wants to make it more difficult for them to access weapons and financial resources. The EU is also trying to get social networking companies to block the content of terrorist messages more quickly. The EU's most pressing "cyber problems" are artificial intelligence (AI) and 5G technology, the next generation of mobile communications. AI algorithms are used for everything from self-driving machines to identifying criminals and can be used for malicious purposes. 5G technology promises to boost connectivity and drive technological innovation, but Chinese companies – which the EU and the US do not trust – are major providers of the underlying infrastructure.

2. Fundamental basic concepts related to the broached topic

The European Commission has approved a legislative package establishing a framework to ensure interoperability between EU information systems in regard to borders, visas, police and judicial cooperation, asylum and migration. The aim of this legislative package is to help support Member States' efforts to combat serious crime at EU level, in particular the fight against identity and document fraud, thus supporting the fight against terrorism and organized crime, as well as the phenomenon of illegal migration.

The Schengen area is a unique European concept, representing an area of freedom of movement without controls at the common borders of the Member States, delimited by a single external border under the administration of the Member States and where border control and surveillance are carried out according to a set of rules established and implemented in a uniform manner. The acquis represents all the rules and measures implemented by the Member States, the decisions, the declarations adopted and the accession agreements of the States, as well as the Schengen Agreement and the Accession Convention.

The concept of "EU information systems" refers to the EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN systems as follows:

- Entry / Exit System (EES) for recording the entry and exit data of third-country nationals crossing the EU's external borders;
- The Visa Information System (VIS) is a tool to support the implementation of the Common European Union (EU) Visa Policy and is intended to enable Schengen States to exchange visa data;
- The European Travel Information and Authorization System (ETIAS) is a fully electronic system that allows and stores tracking of visitors from visa-free countries to enter the Schengen Area;

- The system for comparing the digital fingerprints of third-country nationals (Eurodac), the fingerprint database of asylum seekers used by the EU;
- European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN).

The Schengen Information System (SIS) was designed as a database shared by border and migration authorities, as well as law enforcement authorities in Schengen member and associated countries, and contains information on individuals, and lost and stolen goods. The National Information System for Alerts (SINS) is the information system created at national level. Certain databases in it are intended to be part of the national component of the Schengen Information System (N-SIS). Operation and use of the Schengen Information System - SIS is composed of: the central computer system (located in Strasbourg, France) and the national computer systems, connected to the SIS, which allow the competent national authorities to search the SIS.

SIRENE is the human interface of the SIS and is the only point of contact with the other Member States. The purpose of setting up SIRENE - "Supplementary Information Request at the National Entries" is the need for the exchange of information at the level of all Member States and Schengen Associations, within the framework of international police cooperation between Member States, in accordance with the provisions of the relevant European legislation.

Within the topic you can find concepts such as:

- facial imagery represents digital images of the face;
- biometric data means dactyloscopic data or facial image or both;
- dactyloscopic data means fingerprint images and latent fingerprint images which, due to their uniqueness and the reference points they

contain, allow reliable and conclusive comparisons regarding a person's identity;

- biometric template means a mathematical representation obtained by extracting features from biometric data limited to the parameters necessary to perform identifications and verifications;
- travel document means a passport or other equivalent document which entitles the holder to cross the external borders and to which a visa may be applied;
- a natural or legal person belonging to a State under the protection of another State;
- interoperability is the ability of distinct and diverse organizations to interact in order to achieve mutually beneficial and mutually agreed objectives, involving the sharing of information and knowledge between organizations, through the professional processes they support, using the exchange of data between their systems ICT;
- interoperability framework means a common approach to interoperability by organizations that wish to work together for the joint provision of public services and, within its scope, it specifies a set of common elements such as vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications and practices;
- interoperability solutions represent joint services and generic tools that facilitate cooperation between distinct and diverse organizations; European interoperability reference architecture or "EIRA" is a generic structure that includes principles and guidelines applicable to the implementation of interoperability solutions in the Union.

3. Contributions regarding the operationalization of the submitted research

The implementation of the framework for ensuring interoperability between existing and developing European information systems will lead to streamlining the operational work of the competent national authorities, by facilitating the correct identification of persons and combating identity and document fraud in the Member States, and to the technical provision of continuous, systematic, controlled and easy access to systems, strengthening the security and data protection conditions, as well as improving the data quality requirements applied to those systems.

The new architecture of European information systems, which will be developed with the implementation of interoperability components, will create new infrastructures, established through common services, policies and requirements, technical tools that will allow a secure cross-border exchange of information best characterized as fast, easy, systematic and controlled.

The implementation of the interoperability framework will improve the efficiency of service delivery, while reducing costs, and will ensure the availability of information and improved identity management in European information systems. Interoperability between EU information systems should allow for mutual complementarity in order to facilitate the correct identification of persons, including persons with unknown identities who cannot identify themselves or unidentified human remains, in order to help combat identity fraud, in order to improve and harmonize the data quality requirements set out in those EU information systems.

The role of interoperability components is to process the personal data of persons whose personal data are processed in the EU's basic information systems and by Europol.

The interoperability components of existing or developing EU information systems are:

- a European search portal (ESP);
- a common biometric data comparison service (common BMS);
- a common register of identity data (CIR);
- a multiple identity detector (MID).

The final purpose of the interoperability components is:

- improving the effectiveness and efficiency of external border checks;
- contributing to preventing and combating illegal immigration;
- helping to ensure a high level of security in the Union's area of freedom, security and justice, including the maintenance of public security and order, and ensuring security in the territory of the Member States;
- improving the implementation of the common visa policy;
- facilitating the examination of applications for international protection;
- contributing to the prevention, detection and investigation of terrorist offenses or other serious crimes;
- facilitating the identification of unknown persons who cannot identify themselves or unidentified human remains in case of natural disasters, accidents or terrorist attacks.

The new information system architecture will be based on interoperability components of the following EU operational information systems: Entry / Exit System (EES), Visa Information System (VIS), European Travel Information and Authorization System (ETIAS), the system for comparing the fingerprints of third-country nationals (Eurodac), the Schengen Information System (SIS) and the European Criminal Records Information System for third-country nationals (ECRIS-TCN).

The European Search Portal (ESP) - part of the interoperability information system - aims to facilitate rapid, uninterrupted, efficient, systematic and controlled access by Member States' authorities and Union agencies to EU information systems, Europol data and Interpol databases for the performance of their tasks and in accordance with their access rights and the objectives and purposes of EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN.

In accordance with the current legislation laying down the legal rules for access to EU information systems, access to the European search portal is restricted to the authorities of the Member States and Union agencies having access to at least one of the information systems.

The European Union Agency for the Operational Management of Information Systems (eu-LISA) has the obligation to create a profile, in collaboration with the Member States, in order to make it easier to access the European portal.

Through the European portal each Member State that has created a profile launches a query by transmitting alphanumeric or biometric data. In this situation the portal will query the following functional databases: EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN and CIR, Europol data and Interpol databases simultaneously, using the data transmitted by the user of the European portal and according to user profile.

The main categories of data used to launch a query through the portal correspond to the categories of data relating to persons or travel documents that can be used to query the various EU information systems, Europol data and Interpol databases according to the judicial tools governing them.

Another component of the interoperability information system is the Joint Biometric Data Comparison Service (BMS), which stores biometric templates based on biometric data and allows queries to be used using biometric data in several EU information systems.

Biometric templates are stored in the common BMS in a logically separate form depending on the information system from which the data comes.

For each set of data mentioned, the common BMS includes in each biometric template a reference to the EU information systems, in which the corresponding biometric data and a reference to it are stored in the actual records in the EU information systems.

Another novelty regarding the interoperability component is the common register of identity data (CIR), in which an individual file is created for each person who is registered in EES, VIS, ETIAS, Eurodac or ECRIS-TCN.

The role of the common identity register is to store the following categories of data, logically separated, depending on the information system from which the data comes: name (family), first name, date of birth, place of birth (locality and country), citizenship or nationalities, gender, previous names, if any, aliases or loan names, if available, and, if available, information on travel documents.

The right to interrogation in the common identity register (CIR) shall be exercised by a police authority only in the following circumstances:

- if police authority is unable to identify a person due to the lack of a travel document or other credible document proving the person's identity;
- if there are doubts about the identity data provided by a person;
- if there are doubts as to the authenticity of the travel document or other credible document provided by a person;
- if there is doubt as to the identity of the holder of a travel document or other credible document; or if a person cannot or refuses to cooperate.

Interrogations are not allowed in the case of minors under the age of 12, unless the interrogation is in the best interests of the child.

Another novelty is the fact that there are good reasons to believe that a consultation of EU intelligence systems will contribute to the prevention, detection or investigation of terrorist offenses or other serious criminal offenses, especially if there are any reasonable suspicions that the suspect, perpetrator or victim of a terrorist offense or other serious crime is a person whose data are stored in Eurodac, the designated authorities and Europol may consult the CIR to find out if the data of a particular person are present in Eurodac. In order to support the functioning of the Common Identity Register (CIR) and to support the achievement of the objectives of EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN, a Multiple Identity Detector (MID) is established, that creates and stores identity confirmation files, which contain connections between data from EU information systems included in the CIR and SIS, thus enabling the detection of multiple identities, with the dual purpose of facilitating identity checks and combating identity fraud.

Where the data contained in one of the EU information systems, including biometric data, the CIR and the Central SIS use the common BMS to detect multiple identities. The joint BMS compares biometric templates obtained from any new biometric data with existing biometric templates in the joint BMS to verify that data belonging to the same person are already stored in the CIR or Central SIS.

Multiple identity detection is only launched to compare data available in one EU information system with data available in other EU information systems. MID indicates the authority responsible for manually verifying the different identities in the identity confirmation file. The authority responsible for manually verifying the different identities in the identity

confirmation file is the SIRENE bureau of the Member State that created the alert, if a connection is established between the data contained in an alert.

The European Union Agency for the Operational Management of Information Systems (eu-LISA) is responsible for developing the interoperability of EU information systems, playing a crucial role in implementing the new technical architecture. The Agency, in accordance with the legal provisions issued by the Parliament of Europe and the Council of the European Union, will develop the technical architecture of interoperability components, providing communications infrastructure at central level, connections to Member States and will provide a set of equipment to each Member State. for connection to central systems. The technical management of interoperability components, also provided by eu-LISA, will include all the tasks and technical solutions needed to keep the systems running, providing uninterrupted services to Member States and European Union agencies, 24 hours a day, seven days a week.

Romania as a Member State with full rights in the European Union has the obligation to implement the new architecture of European information systems and interoperability components. The authority designated according to the internal regulations of the headquarters is the Ministry of Internal Affairs for the 5 information systems it manages, and the Ministry of Foreign Affairs for a system. In order to implement without syncope, taking into account that the legislative package covers activities and obligations in the operational field of police, border police, asylum, migration, visas, a need to adapt was identified, adapting through national legislation some provisions of regulations, a process currently under the analysis and elaboration phase at the level of the competent authorities. In order to monitor compliance with the provisions of the European regulations establishing information systems and the interoperability framework at their level, a Steering Committee for the new architecture of European border and

security information systems has been set up. The implementation of the new architecture of the European information systems in Romania will represent a new approach towards the way of working and the activity of the law enforcement authorities that will use these new tools.

For the new architecture of the EU's information systems to be effective in a world of mobility, it is necessary to apply a new framework on enhancing the security of Union citizens' identity cards and residence documents issued to Union citizens and their family members who exercise the right to free movement. There are currently significant differences between the security levels of national identity cards issued by Member States and those of residence permits for Union citizens residing in another Member State and their family members. These differences increase the risk of forgery and fraud of documents. Statistics from the European Document Fraud Risk Analysis Network show that the number of identity card fraud cases has increased. According to the Regulation, the Parliament of Europe and the Council of the European Union need to include security features in order to verify that a document is authentic and to establish a person's identity. Setting minimum security standards and integrating biometric data into the identity cards and residence permits of family members who are not nationals of a Member State are important steps to make the use of these documents safer in the Union. The inclusion of these biometric identifiers should enable citizens to fully enjoy their rights to free movement.

Storing a facial image and two fingerprints (hereinafter referred to as "biometric data") on identity cards and residence permits, as already provided for passports and biometric residence permits of third-country nationals, is an appropriate method to associate reliable identification and authentication with a low risk of fraud, in order to enhance the security of identity cards and residence permits.

The electronic identity card (CEI) will allow the holder to authenticate in computer systems of the Ministry of Internal Affairs and in computer systems of other public or private institutions, as well as the use of the electronic signature, in accordance with the law. The identity card will thus facilitate the citizen's access to various electronic services (banking, tax, social, financial, etc.), with major effects on simplifying the relationship with public authorities, increasing the quality and accessibility of public services. The electronic identity card will comply with the requirements of the European Commission on the security of documents, in the context of the fight against terrorism, illegal migration, drug and human trafficking, the current identity cards being made with technology from the '90s. The new identification document will provide citizens with additional security guarantees, and public or private law institutions the certainty that the person presenting the identity document is the holder of the identification data entered on that document.

4. Final conclusion

We believe that the new information systems architecture and interoperability components will in particular ensure the operational needs of border guards, police officers and other law enforcement institutions by facilitating access to accurate information and combating identity fraud while offering from a technical point of view fast, continuous, systematic and controlled access.

At present, EU information systems do not communicate effectively because information is stored separately in disconnected systems and is difficult to operate. There is thus a risk that valuable information will be lost. Identifying technical solutions in data management and improving the interoperability of existing or developing information systems must be a priority for the Member States of the European Union to ensure the security

of the individual at the heart of the Security Union, rather than the security of the Member States. The interoperability of data systems in the field of structures within the Ministry of Internal Affairs (Police, Border Police, etc.), has as main attribute the much faster identification of cases of identity theft or multiple identity that may pose a threat to security or which are used for committing serious crimes such as human trafficking, acts of terrorism, drug trafficking and consumption, arms trafficking.

We believe that in order to identify persons who pose a security threat or who do not provide sufficient data to establish their identity, the competent authorities carrying out the checks must have a complete picture of the person in front of them. The interoperability components and the new information systems architecture will allow authorities to query all information stored in existing databases and compare biometric data from these common databases to identify multiple identity cases. This technical framework aims to operationalize and implement interoperability components by interconnecting existing data with a single click through a European search portal aimed at detecting identity theft or multiple identities. In this way, border guards and police officers will be able to better identify dangerous criminals thanks to the common biometric matching service, which will use fingerprints and facial images to search existing computer systems.

The product of interoperability can be observed every day at EU borders, during border checks or border surveillance, and in joint operations. It plays a crucial role in setting up the operational environment for border guards, reflecting their ability to act and operate together.

We consider that innovation in the field of borders must ensure a high standard of security at the external border of the European Union and that new technologies must be seen as elements that support the personnel serving the structures of the border police.

References

Camino, M., (2019). *The EU's Security Union: a bill of health*

Decision (EU) 2015/2240 of the European Parliament and of the Council of 25 November 2015 establishing a program on interoperability solutions

Jeffray, C., (2017). *Fractured Europe: The Schengen Area and European border security (pp. 7-9, Rep). Australian Strategic Policy Institute.Ret*

Law no. 162 of 03 August 2020 regarding chip identity cards

Law no. 141 of 12 July 2010 (* republished *) on the establishment, organization and functioning of the National Information System for Alerts and Romania's participation in the Schengen Information System

Niklas, N., (2019). *EU's new Security Union Strategy is a good first step*

Parkes, R., (2015). *European Union Institute for Security Studies (EUISS)*

Regulation no. 129/2019 of 13 November 2019, on the establishment, at the level of the Ministry of Internal Affairs, of the Steering Committee of the new architecture of European information systems for border and security

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

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

Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement; Schengen Border Codes, instated through Regulation (EU) 2016/399

The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders

https://www.consilium.europa.eu

https://epso.europa.eu

https://www.gov.ro

https://dexonline.ro

Instructions for authors

Review of Management General is published in English.

All articles are evaluated in the "peer review" system.

Material size has to be of 7-15 pages.

The articles can be sent by internet at the address:
redactie_rmg@yahoo.com

The authors are not allowed to insert page numbers and or any header or footer element within the paper, except footnotes, which are part of the paper.

The authors are fully responsible for the whole content of the paper and for the quality of the phrases and sentences used either.

For any other information, visit our website: ***www.managementgeneral.ro***

REVIEW OF GENERAL MANAGEMENT
SUBSCRIPTION ORDER FORM

Subscription for **2020**

I would like to receive the journal at the following address:

Last name, first name (company/organization)_____

Address_____

_____

Telephone_____ fax _____

E-mail _____

Payment details: **Account no. IBAN: RO93RNCB0074029222760001,** opened at **BCR, sector 3, Bucureşti, România. Beneficiary: Editura Expert. Please specify** „for **Review of General Management**".

Please send this subscription form, after filling it in, and a copy of the payment document by mail (**redactie_rmg@yahoo.com**), at the following address: Universitatea *Spiru Haret*, Facultatea de Management, Braşov, str. Turnului nr. 7, cod 500152, România.

The subscription rate: **150 lei/year.**

TALON DE ABONAMENT

REVIEW OF GENERAL MANAGEMENT

Abonament pe anul **2020**

Doresc să primesc abonamentul la adresa:
Nume şi prenume (societatea) _____
Adresa _____
_____
Telefon _____ fax _____
E-mail _____

Contravaloarea abonamentului se va achita în contul Editurii Expert, la **BCR, sector 3, Bucureşti, cont IBAN: RO93RNCB0074029222760001,** cu menţiunea „pentru **Review of General Management**".

Vă rugăm să trimiteţi talonul completat împreună cu dovada plăţii prin email (**redactie_rmg@yahoo.com**) sau prin poştă la adresa: Universitatea *Spiru Haret*, Facultatea de Management, Braşov, str. Turnului nr. 7, cod 500152, România.

Costul unui abonament: **150 lei/an.**