REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the implementation of the Action Plan to strengthen the EU response to travel document fraud

I. INTRODUCTION

The Commission adopted on 8 December 2016 a Communication on an Action Plan to strengthen the European response to travel document fraud aiming at improving the overall security of travel documents issued in the EU (hereinafter Action Plan)[1]. The Action Plan addressed the increasingly significant problem of travel document fraud, which became more relevant in the context of the terrorist attacks and migration flows. Against this background, it was crucial that the EU and especially the Member States intensify efforts to improve the security of travel documents, thus contributing to better border protection and migration management and to move towards an effective and genuine Security Union.[2]

The Action Plan looked at concepts and processes to manage identity, identified actions to close potential loopholes for Member States, the Commission, the Council and the European Parliament.

This report provides an overview of the results and progress made on a number of work strands and specific measures undertaken by the Member States, the European institutions and other stakeholders to fulfil the actions described in the Action Plan. Furthermore, Council Conclusions on the Action Plan were adopted on 27 March[3] and on identity management on 18 December 2017[4] calling on Member States to take action towards enhancing the integrity of national identity systems.

The report follows the structure of the Action Plan thus showing the progress made in each of the key areas of the identity infrastructure: registration of identity, issuance of documents, document production and document control.

II. REGISTRATION OF IDENTITY

Registration or evidence of identity refers to processes enabling the tracing, linkage and verification of identity against breeder documents (e.g. birth certificates) to ensure that the individual's identity is legitimate, authentic and living.

Registration processes fall under Member States' responsibility. The Council Conclusions of 27 March 2017 highlight the importance of more secure breeder documents to prevent fraud when used as evidence of identity, while the Council Conclusions of 18 December 2017 stress the importance of support to key third countries on the introduction of biometric identifiers in their population registers.

The Commission has facilitated discussion on identity management and assessed the situation in Member States, notably by presenting a **questionnaire** under the Maltese presidency[5] on issues regarding the registration of identity and supporting the organisation of a thematic

---

[1]   COM(2016) 790 final.

[2]   Commission Communication on delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union (COM(2016) 230 final, 20.4.2016).

[3]   Council conclusions on the Commission action plan to strengthen the European response to travel document fraud - http://www.consilium.europa.eu/en/press/press-releases/2017/03/27/jha-travel-document-fraud/

[4]   Council conclusions on identity management - Doc 15862/17 of 18 December 2017.

[5]   Council Doc. 12004/17 of 30 January 2017.

meeting on the same topic. In particular, the questionnaire addressed breeder documents, taking of biometrics for population registers, name changing procedures and other identity-related issues. The **assessment** took place under Estonian presidency[6] and showed that Member States' practices diverge in this area. Member States should continue to exchange national practices and to assess how procedures in other Member States[7] can serve as examples for improving national processes, notably procedures to improve the security of breeder documents and registering identity of citizens (e.g. online registration; registration of identity during adulthood and taking of biometrics for population registers).

Furthermore, the thematic False Documents working party meeting held on 16 November 2017 provided different perspectives on issues related to registration of identity from the global ICAO[8] approach on evidence of identity to the OSCE[9] regional approach presented in its *Compendium of Good Practices in Identity Management* launched in September 2017. It also included Member States input about their national practices and the findings of the ORIGINS[10] and ARIES[11] projects.

The OSCE Compendium collects and assesses evidence of diverse identity registration practices in the OSCE countries (which includes all EU Member States) and serves as guide on capacity building efforts. Overall, the EU and the OSCE assessments are key for EU Member States to compare their own systems, use it to identify potential weaknesses and reflect on how the different practices can serve as examples for improvement.

As a follow up, the **Council adopted conclusions on identity management** on 18 December 2017, which prioritise continued cooperation and information exchange among Member States to align practices and further improve the integrity of national ID systems, while emphasising the need for robust and sound identity infrastructures to efficiently mitigate security risks.

Regarding the **international dimension** of the Action Plan on the introduction of biometrics in the population registers of key third countries, the Commission engaged in dialogues with Mali and Senegal, both of which are already implementing EU Trust Fund projects on civil registries since early 2017. Based on cooperation and technical support, other ongoing actions with key partner countries include Tunisia, Niger and Sudan. Countries that express interest on possible civil registries projects may also benefit from technical support depending on available funding and the priorities set out to address new eligible countries.

The **Europol's Handbook on breeder documents** lists Member States' breeder documents, describes briefly their issuing processes and provides a list of national contacts points. The handbook should allow document-issuing authorities to better detect false documents. The handbook is still being finalised but an interim version is accessible online in FADO[12] system

---

6   Council Doc. 12004/1/17 of 27 November 2017.
7   The Rotterdam declaration following the "Cross Border by Default" conference, organised by the Dutch National Office for Identity data on 11-12 April 2016 attached particular importance to the value of sharing practices in the area of population registries.
8   International Civil Aviation Organisation,
9   Organisation for Security and Co-operation in Europe,
10   ORIGINS: 'Recommendations for Reliable Breeder Documents Restoring e-Passport Confidence' and 'Leveraging Extended Border Security'.
11   ARIES: 'Reliable European identity ecosystem'.
12   FADO is the summary name for a trio of information and technology systems: Expert FADO, iFADO (Intranet FADO) and PRADO (Public Register of Authentic Documents Online). It is a European image

and through the Europol Platform for Experts directed at law enforcement specialists. Together, these two platforms reach out to a wide community, including law enforcement agencies and some issuing authorities such as consular staff, passport and immigration authorities.

Regulation (EU) 2016/1191 of 6 July 2016 on promoting the free movement of citizens by simplifying the requirements for presenting certain public documents in the European Union will become applicable on 16 February 2019. Under this Regulation, public documents, such as birth certificates, issued in a Member State and presented to the authorities of another Member State will be exempt from the apostille stamp. The Regulation will strengthen the fight against fraudulent public documents by enabling the authorities in the receiving Member State, if they have doubts about the authenticity of the public document presented, to consult the issuing authority through the Internal Market Information system. .

Regarding **Research & Development activities** on breeder documents and document verification including mobile technologies, the Commission financed three main projects in the framework of the Horizon 2020 programme for Secure Societies: ORIGINS, which finished mid-2017, FIDELITY[13] concluded in 2015 and ARIES launched in 2016. These research projects address aspects related to combating ID fraud, protection of existing identities, image morphing[14] and fingerprint spoofing. Follow-up activities include continuity of the ORIGINS project through the European Committee for Standardisation (CEN) WG19[15] on breeder documents standardisation; a consortium on an image morphing research program; the SIRIUS[16] project aiming at capturing standardised reference data from documents and ENLETS Mobile[17], which looks into new developments and shares good practices on mobile solutions for front line law enforcement officers.

III. ISSUANCE OF DOCUMENTS

Document issuance refers to processes and protocols for issuing a document to legitimate holders and the controls to prevent theft, tampering and loss of documents while issuance is taking place.

Issuance of documents falls under the responsibility of Member States. Work is ongoing on establishing a **best practice guide for the correct enrolment of biometric identifiers**, which looks into face and fingerprints biometric enrolment and stresses the importance of live enrolment of facial images to efficiently combat identity fraud through image morphing. It

---

archiving system, set up to assist Member States in managing and recognising authentic and false documents. Subsystem iFADO is intended for law enforcement and document issuing authorities, while PRADO subsystem, available via internet, aims at the 'non-document expert' community.

[13] FIDELITY: 'Fast and Trustworthy Identity Delivery and Check with ePassports Leveraging Traveller Privacy'.

[14] Image morphing is an image processing technique used to produce an artificial biometric sample (i.e. morphed image) which resembles the biometric information of two or more individuals...

[15] European Committee for Standardisation/ *Comité Européen de Normalisation* working group 19 on machine-readable travel documents (CEN TC224/WG19).

[16] SIRIUS: Secure ID documents Reference and Inspection support User assistance System.

[17] ENLETS Mobile is a subgroup of the European Network of Law Enforcement Technology Services (ENLETS), which reports to the Law Enforcement Working Party (LEWP) in the Council.

also addresses biometric data quality and highlights practical challenges and lessons learned[18]. This work is supported by CEN, which will establish a technical standard for enrolment of biometric identifiers together with Member States' experts in the Article 6 committee[19]. For its part, eu-LISA[20] started developing common data quality indicators and minimum quality standards for the correct enrolment of biometric data stored in EU databases.

Concerning **best practices on document issuance procedures and implementation of the Council conclusions adopted in 2005[21] on minimum standards as regards the security of issuing processes**, the Bulgarian presidency established a questionnaire[22] on issuing related processes, which revealed that all Member States are broadly compliant with those standards.

In the framework of the Visa and Residence permit subgroup of the Art 6 committee, technical discussions led to agreement on **allocating a unique number to all document products** before they leave production premises. This procedure will enable entering traceable descriptors of lost/stolen document components in relevant systems, and will limit the number of blank stolen items in general.

IV. DOCUMENT PRODUCTION

Document production refers to the designing and manufacturing of secure, standardised and globally interoperable documents. ICAO governs the standards for globally interoperable travel documents by setting out the specifications for (electronic) machine-readable travel documents (MRTDs and eMRTDs).

The Commission is responsible for setting out the security standards and biometrics for travel documents issued to EU citizens and third country nationals living in Member States' territory. A major outcome in this area concerns the adoption in 2017 of the **Commission's proposals on a more secure uniform format for visas[23] and residence permits for third country nationals[24]**. The Commission adopted the implementing decision on technical specifications for the uniform format for visas[25], while the one on the residence permits is planned for the end of 2018.

Equally essential was the resumption of the technical support from the JRC to **verify the correct implementation by Member States of the physical and electronic features as**

---

[18]   JRC Technical Report, Automatic fingerprint recognition: from children to elderly, Ageing and age effects, EUR 29265 EN, 2018, ISBN 978-92-79-87179-5, doc 10.2760/809183.

[19]   The committee created by Article 6 of Regulation (EC) 1683/95 laying down a uniform format for visas.

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

[21]   Conclusions of the Representatives of the Governments of the Member States on common minimum security standards for national identity cards (1-2 December 2005).

[22]   Council Doc. 9231/18 of 31 May 2018.

[23]   Regulation (EU) 2017/1370 of the European Parliament and of the Council of 4 July 2017 amending Council Regulation (EC) No 1683/95 laying down a uniform format for visas.

[24]   Regulation (EU) 2017/1954 of the European Parliament and of the Council of 25 October 2017 amending Council Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third country nationals.

[25]   Commission Implementing Decision C(2018) 674 of 12 February 2018 as regards further technical specifications for the uniform format for visas and repealing Commission Decision C(2010) 319 of 27 January 2010.

required by EU legislation for passports, residence permits and the uniform format for visas. While the complete testing should be finalised in the first quarter of 2019, the interim report was delivered in April showing good progress. Once the testing phase is finalised, the Commission will assess the need for further steps in cases of non-compliance with the established standards. Furthermore, the Commission organised an interoperability test event for electronic passports and residence permits in September 2017 at the JRC premises. This event successfully assessed the compliance of travel documents with global interoperability standards in Member States as well as some other ICAO contracting states.

The Commission adopted on 17 April 2018, a legislative initiative to **strengthen the security of identity cards of Union citizens and of residence documents issued to Union citizens and their non-EU family members exercising their right of free movement**[26]. This proposal seeks to facilitate the exercise of citizens' right to free movement and to improve the overall security of such documents. The Commission proposed minimum document and security standards for ID cards, minimum information to be provided on residence documents issued to mobile EU citizens and full harmonisation of residence cards issued to non-EU family members. The proposal provides for a fast phasing-out of cards that do not comply with the proposed standards, in order to reach fast progress on overall document security. The proposal is currently under discussion by the co-legislators with the aim of being adopted during the current legislative cycle.

Furthermore, in its EU citizenship report 2017, the Commission committed to exploring possibilities to **modernise the rules on emergency travel documents (ETDs)** including the security features of the EU common format[27]. On 31 May 2018, the Commission adopted a legislative proposal introducing new rules on an EU ETD with enhanced security features[28], which is currently under discussion by the Council and the Parliament.

The Commission looked into the issue of the **non-inclusion of the local border traffic permits (LBT) in the ETIAS[29] system and assessed the security risk**. The conclusion was that there is no need to amend Regulation (EC) No 1931/2006 because it already provides that LBT permits' security features be automatically aligned with any upgrade of residence permits for third country nationals as provided for in Regulation (EC) 1030/2002. In this respect, it should be noted that the security features of residence permits for third country nationals have been upgraded recently pursuant to Regulation (EU) 2017/1954.

V. DOCUMENT CONTROL

Document control deals with processes aiming at the efficient and secure reading and verification of travel documents. It also covers those processes enabling the timely, secure and reliable linkage of documents and their holders to available and relevant data in the course of inspection operations. Likewise, it includes training and data assessment

---

[26] COM(2018) 212 final.
[27] Decision 96/409/CSFP of the Representatives of the Governments of the Member States, meeting within the Council of 25 June 1996 on the establishment of an emergency travel document.
[28] COM(2018) 358 final - Council Directive establishing an EU Emergency Travel Document and repealing Decision 96/409/CFSP.
[29] European Travel Information and Authorization System.

mechanisms, which allow for the correct use of systems (document readers, databases, equipment etc.) and help in the process of taking informed decisions.

A major step forward in this area was the Commission's proposal on the **new legal basis of the Schengen Information System (SIS)** adopted on 21 December 2016, which provided for enhancing its functionalities, including allowing Member States to enter falsified travel documents in the system and proposing to make the implementation of fingerprint functionality mandatory if the identity of the person cannot be ascertained otherwise. Political agreement has been reached and adoption is planned for the end of 2018. In the meantime, eu-LISA and the Member State have successfully launched on 5 March 2018 **the Automated Fingerprint Information System (AFIS),** enabling a fingerprint search functionality at central level in Schengen Information System (SIS). The SIS AFIS is the first centralised European wide criminal fingerprint database and is a major milestone for the European security allowing for the detection of criminals using multiple or fraudulent identities. Seven Member States implemented the direct search with fingerprints in SIS, which is expected to be extended to almost 20 by the end of 2018. eu-LISA has also delivered a feasibility study enabling cross-matching of biometrics across all of its IT systems which will be taken into consideration for future developments of the systems.

Discussions have been concluded in SISVIS committee on how to enforce the **seizure of stolen, lost, misappropriated or invalidated documents.** The Commission updated the 'Catalogue of recommendations and best practices on the use of the Schengen Information System' providing, by way of guidance, a set of indicative criteria in relation to the seizure of documents, aiming for a more harmonised approach among Member States.

Regarding the **systematic feeding of Interpol databases with data on Stolen and Lost Travel Documents (SLTD),** issued by non-EU countries, where those countries are not able to do so themselves, the Commission is financing projects[30], which will include support to deploying Interpol tools (including SLTD) in a number of Middle East and North African countries. This ongoing process will improve third countries' capacity to enter data in SLTD by themselves.

Furthermore, since 7 April 2017, **systematic checks against relevant databases** for all travelers crossing the external borders are in place. Those databases, which are mandatory for consultation, include the SIS and Interpol's SLTD. Together with the work the Commission is doing on enhancing the information fed into the SLTD, the SIS and other document databases, it will increase document security.

The above-mentioned Council Conclusions of 27 March 2017 also stressed the need to accelerate the implementation of the **exchange of certificates for the checking of fingerprints** through Single Points of Contact (SPOC) and the authentication of the chip data using a Masterlist.

Regarding the **list of certificates needed for the electronic authentication of travel documents**, the Commission published on 20 December 2016 the first Schengen test **Masterlist** and launched a border control pilot-test with Norway and Portugal in the first semester 2017. Work is also in progress regarding contacting third countries for receiving

---

[30]   Project SHARAKA.

their passport certificates. The Commission began work to create and update an official Masterlist, signed with the key of the EU Laissez-Passer Country Signing Certificate Authority (CSCA), for which the authorisation has been obtained. The Commission is reflecting on the necessity of a legal instrument regarding a "masterlist policy", which will allow determining when a third country certificate can be added to the list.

On the use of biometric applications for document security and the exchange of certificates, Member States SPOCs enable the automated bilateral secure exchange of the certificates required to read the fingerprints in travel documents. The progress towards the transition from test to fully operational SPOCs in the Member States, is monitored by the Commission on a monthly basis. Currently ten Member States and Schengen associated countries are fully able to exchange certificates and check fingerprints on operational systems on citizen's documents while 21 are still in testing phase. The Commission urges Member States to actively engage in making the exchange of live certificates operational in the shortest delay possible.

As regards the measure **to ensure better access to the relevant information systems**, recital 6 of Regulation (EU) 2017/458 amending Schengen Borders Code calls on Member States to ensure border guards have access to relevant databases at the border crossing points. Furthermore, Art.40(8) of the European Border and Coast Guard Agency (EBCGA) Regulation sets out that the host Member States shall authorise the members of the EBCGA teams to consult European databases which is necessary for fulfilling the operational aims of border checks, surveillance and return. Likewise, legislative proposals for amending the Visa Information System[31] and the SIS regulations for border control and for police cooperation, which are under discussion, include provisions for granting EBCGA access. Furthermore, from an operational perspective, the Commission included in the Internal Security Fund - Police 2017 Annual Work Program: a direct award to Interpol to deploy its technology to a selected number of Member States in order to increase their use of SLTD and other Interpol databases, and a call for proposals restricted to Member States to increase the use of SLTD and other Interpol databases at the external EU border crossing points.

Drafting a technical report on standards for inspection systems is ongoing. In support of this activity, EBCGA is developing a methodology for testing and assessing the performance of Document Inspection Systems. The work started in April 2018 and includes operational testing against document inspection systems in real-life border control scenarios in the third quarter and the final report by the end of 2018. The results of the performance assessment methodology for document inspection systems activity will feed into the technical report on inspection systems of the technical subgroup of the Article 6 committee. Progress will much depend on the outcome of the above-mentioned EBCGA performance assessment activity and on the engagement of Member States.

A key achievement is the enhanced operational support provided by the **EBCGA Centre of Excellence for Combating Document Fraud**, launched in February 2018. This Centre deploys EBCGA staff to field operations at the external borders, contributes to **information exchange on document fraud** and plans setting up a **Forgery Desk** providing permanent

---

[31] COM(2018) 302 final - Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA.

technical and operational support to document control. The Centre also manages the **Expert Group on Document control,** aiming at coordinating overall support to Member States in detecting document fraud, and works closely with the **Horizontal Expert group on Document fraud** created in the framework of the EU Policy Cycle 2018-2021[32] to disrupt networks of criminal organisations trafficking in false and falsified documents. The Centre is finalising a new proposal for a standardised format for alerts[33] planned for the end of 2018.

Furthermore, on **improving data collection on document fraud phenomena,** EBCGA maintains the European Union Document Fraud - Risk Analysis Network (EDF-RAN) and collects information on both document and identity fraud detected at the external EU borders and intra-EU/Schengen movements. EBCGA also develops and updates publications on specific documents and fraud-related issues. Looking ahead, EBCGA will enhance data quality and expand the EDF-RAN data collection scope to include, e.g. fraudulent documents presented during visa applications and pre-boarding denials.

Regarding **new document fraud phenomena**, EBCGA addressed **image morphing** in its 2017 train-the-trainer course on "Vulnerability assessment and testing for Automated Border Control systems" and also in the 2017 Handbook on Impostor Risk Profiles. EBCGA continues to work on improving training and awareness tools.

In terms of **promoting training activities in new areas of document fraud**, **EBCGA** in partnership with the Academy Eindhoven–ID Centre, developed a pilot course on identity expertise, which includes reference to identity management, chip technology, biometrics and means to detect digital fraud. A second edition is planned for 2018. Likewise, EBCGA is developing a specific module on breeder documents and is updating the programmes of its training portfolio, spanning from specialised trainings to awareness raising events, such as roadshows, assistance to third countries, webinars and training sessions for consular staff. In this domain, the Commission, in partnership with EBCGA organised a series of six workshops in key locations abroad[34] aimed at assisting EU consular officials with the detection of false documents submitted for EU visa applications. For its part, **CEPOL**[35] provides trainings, webinars and exchange programmes for officials on document fraud.

With reference to international stakeholders, discussions are ongoing between the International Centre for Migration Policy Development, The Netherlands and the Commission over potential use of the new Mobility Partnership Instrument to tackle the underreported area of smuggling by air and possibly to support targeted document fraud training at high-risk airport locations.

Regarding the **assessment of the feasibility of a proposal to amend or revise the Carriers Liability Directive**[36] to include training requirements, there are no plans to amend this

---

[32] EU Policy Cycle for organised and serious international crime/ **E**uropean **M**ultidisciplinary **P**latform **A**gainst **C**rime **T**hreats (**EMPACT**) 2018-2021.

[33] Earlier reference is doc 5606/11 of 27 January 2011 – "Proposal for the setting up of a standardised format for national alerts on false identity and travel documents for national use and for distribution to third countries".

[34] Moscow (Nov 2017), New Delhi, (Jan 2018), Nairobi (Feb 2018), Islamabad (March 2018), Beijing (May2018), Abu Dhabi (June 2018).

[35] European Union agency for Law enforcement training.

[36] Council Directive 2001/51/EC of 28 June 2001 supplementing the provisions of Article 26 of the Convention implementing the Schengen Agreement of 14 June 1985.

Directive in the near future. Further discussion is needed to establish if training for carriers could not be promoted by other means.

As to **improving the use of the False and Authentic Documents Online database (FADO)** and as a follow up to the Council Conclusions of 27 March 2017, the Commission has proposed that the EBCGA takes over and operates the FADO system[37].

Given that the FADO/PRADO platform is accessible to non-document expert community, the discussions on the future of FADO should also include measures on **improving the availability of information on new and false documents to the 'non-document-expert community'**. The access of the non-document expert community to such information is also explored in the context of the R&D projects, notably the ones related to mobile technology.

VI. CONCLUSIONS

The Action Plan has increased **visibility of the issue of travel document security and its underlying identity management infrastructure**. Member States have supported this holistic approach. Progress made include exchange of information on national identity practices and enrolment process of biometrics, enhancement of the security features of the uniform visa and residence permit formats and ongoing discussion to improve the security of ID cards. More secure management of travel documents and better control will contribute to enhance border protection, migration management and to move towards an effective and genuine Security Union.

Security standards for travel documents including biometrics and border control requirements are set at EU level, while Member States retain full responsibility for the breeder documents and for producing and issuing the documents. **Shifting the focus from the actual documents on to the upstream and downstream processes is a logical step to take**.

Out of a total of thirty-two proposed measures in the Action Plan about half of them have been completed and the remaining ones, largely falling under Member States' competence, are either long term or will be implemented in the coming months. Information sharing and exchange of best practices should continue to help Member States identifying loopholes and serve as incentive for introducing changes in the national identity infrastructures.

All this proves the successful impact of the Action Plan, but also shows the need for Member States to continue ensuring all necessary steps to **swiftly implement the remaining measures of the Action Plan and engage proactively in cooperating and improving EU wide information sharing**. Ultimately, Member States should continuously assess and challenge their own processes, seeking to improve efficiency and security across the entire identity chain.

In particular, the **Commission calls on Member States to swiftly implement the measures described in the Council conclusions of 27 March and 18 December 2017**, notably on improving information sharing mechanisms and administrative cooperation to enhance the integrity of national identity related processes; improve the security of breeder documents and

---

[37] COM(2018) 631 final of 12 September 2018.

align best practices in the EU, in full respect of fundamental rights standards, especially with respect to personal data protection. The Commission will continuously monitor the progress and remains committed to facilitate discussion and cooperation in this area.