EUROPEAN
COMMISSION

Brussels, 8.12.2016
COM(2016) 790 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Action plan to strengthen the European response to travel document fraud

I. INTRODUCTION

The increasingly significant problem of travel document fraud has come under the spotlight in the context of the recent terrorist attacks in Europe and current migration flows. Document fraud has become an enabler of terrorism and organised crime, and is linked to the trafficking of human beings[1] and migrant smuggling. It is vital that we enhance the security of travel documents, including the underlying identity management infrastructure.

In its Communication on *Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders*,[2] the Commission stressed the crucial importance of secure travel and identity documents wherever it is necessary to establish beyond doubt a person's identity and announced that it would be presenting an action plan to tackle the phenomenon of travel document fraud. An improved approach will rely on robust systems to prevent abuses and the threats to internal security arising from failings in document security.

Most commonly, travel documents take the form of passports, but they also include national identity cards and residence permits for third country nationals (when used within the area without controls at internal borders). EU citizens can enter and leave the EU, the Schengen area and certain non-EU countries with a national ID card issued by Member States. This means, for example, that foreign terrorist fighters may be able to travel between the EU and Turkey using just their national ID card.

EU travel documents are in high demand among fraudsters. At least three quarters of fraudulent documents detected at the external borders, but also in the area without controls at internal borders, purport to have been issued by EU Member States and the Schengen associated countries.[3] According to recent reports from the European Border and Coast Guard, less secure national ID cards issued by Member States are the most frequently detected false documents used for intra-Schengen travel. 'Look-alike fraud' (where the holder of a document is simply a look-alike of its real owner) is still on the rise and remained the most frequently reported type of fraud in the second quarter of 2016. Obtaining authentic documents on the basis of false 'breeder' documents (birth, marriage and death certificates) remains one of the biggest threats, as it is very difficult to detect.

Against this background, it is crucial that the EU and especially the Member States intensify efforts to improve the security of travel documents issued to EU and third country nationals. Travel document security is an important factor in better border protection and migration management and the move towards an effective and genuine Security Union.[4]

The nature of travel document fraud is evolving rapidly. Criminal networks involved in the falsification and counterfeiting of travel documents are now more specialised and are constantly developing new forms of forgery, such as the manipulation of anti-forgery devices and techniques to circumvent biometric checks, and new *modus operandi*.

---

1 Staff working document SWD(2016) 159 final accompanying the Commission's *Report on the progress made in the fight against trafficking in human beings* (2016).

2 COM(2016) 602 final, 14.9.2016.

3 In the second quarter of 2016, 74.33 % of false ID cards, 60.46 % of false residence permits and 17.11 % of false passports were EU documents (European Border and Coast Guard's quarterly risk analysis report).

4 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).

The introduction of more sophisticated security features, production methods and document inspection systems is making it more difficult to forge or counterfeit identity and travel documents. In response, however, fraudsters are increasingly shifting from 'traditional' fraud – which focuses on the physical document, for example by altering the date of validity in a passport (forgery) or producing a totally fake document (counterfeit) – to other types of document fraud, such as look-alike fraud. They are also targeting other types of documents, such as the breeder documents used to support applications for genuine travel documents.

According to the European Border and Coast Guard's 2016 report,[5] impostor fraud and the fraudulent obtaining of genuine documents increased by 4 % and 76 % respectively between the first quarter of 2015 and the first quarter of 2016, whereas fraud with counterfeit documents decreased (-8 %).

This Communication sets out an action plan to improve the security of travel documents. Security standards for travel documents and border control requirements[6] are set at EU level, but Member States retain full responsibility for the breeder documents and actually producing and issuing travel documents. The action plan sets out measures which the Commission will take and makes recommendations for Member State action under national policies on all aspects of travel document security.

The Commission and Member States have to ensure that fundamental rights in particular the right to personal data protection, will be guaranteed in all measures referred to in this action plan.

As guardian of the Treaties, the Commission will continue to monitor the correct implementation of EU law and use its powers to enforce correct implementation where appropriate and necessary.

II. ACTION PLAN

1. Registration of identity

Authentic documents established on the basis of a false identity are very difficult to detect at border crossings or within a Member State's territory. Individuals' identity should be established, and 'breeder documents'[7] issued, on the basis of population registers containing relevant up-to-date historical, social and geographical data. Countries with a biometric population register or travel document database can check a person's identity each time s/he applies for a new travel document, so a person cannot apply for an authentic document using a false breeder document.

While it can be legal for a person to change his or her name, close attention needs to be paid to this process and the procedures must be watertight. Where adults are registering or applying for a passport for the first time (e.g. following naturalisation) and no reliable registration data are available, the authorities responsible should conduct face-to-face interviews and, as appropriate, look for additional evidence that the person actually uses the claimed identity, for example, via electoral rolls or social security records.

---

5 http://frontex.europa.eu/publications

6 As regards border control requirements see Title V, Chapter 2 of the Treaty on the Functioning of the European Union (TFEU).

7 Breeder documents are birth, marriage and death certificates used to support applications for identity, residence and travel documents.

In addition, breeder documents should have a minimum security level to prevent falsification. The EU has contributed a total of EUR 16 million to research and development initiatives[8] to ensure more secure breeder documents. Future Horizon 2020 work programmes on Secure Societies 2018-2020 will support R&D on document security.

Beyond the EU, there are projects in the framework of the new Partnership Framework under the European Agenda on Migration to develop biometric registration databases in key partner third countries with capacity to ensure functioning civil registries and fingerprint or biometric digitalisation.

Europol has funded the development of a handbook on the detection of false breeder documents. It contains samples and short descriptions of European ID documents and breeder documents, but it is not used as much as it should be.

Electronic identification and trust services for electronic transactions,[9] can also help in the detection of false documents and enhance electronic document security by providing evidence of identity and preventing ID fraud through the mutual online validation of identity data. They would also support the facilitation of secure online applications for the renewal of travel documents.

A recently adopted Regulation simplifying the circulation of public documents in the Union[10] establishes that birth and marriage certificates issued in one Member State can be accepted as authentic in another without an authentication stamp. This strengthens the fight against fraud by introducing administrative cooperation whereby Member States communicate with each other, via the Internal Market Information (IMI) system, in cases of doubt as to the authenticity of a public document, for example, to check the authenticity of breeder documents.

Specific actions
Member States should: - consider how best to avoid issuing authentic documents based on false identities, for example through reinforcing procedures in cases of later-in-life registration of identity/first-time applications or name-changing; - examine how their breeder documents can be made more fraud-resistant, e.g. by adding security features; - ensure wide distribution of the Europol handbook on breeder documents to all

[8] Two projects funded by the FP7 Security Theme relate specifically to document security and ID management: 'Fast and trustworthy identity delivery and check with e-passports leveraging traveller privacy' (Fidelity) and 'Recommendations for reliable breeder documents restoring e-passport confidence and leveraging extended border security' (Origins). The Horizon 2020 Secure Societies Challenge is funding the 'Reliable European identity ecosystem' (Aries) project.

[9] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73–114).

[10] Regulation (EU) 2016/1191 of the European Parliament and of the Council of 6 July 2016 on promoting the free movement of citizens by simplifying the requirements for presenting certain public documents in the European Union and amending Regulation (EU) No 1024/2012 (OJ L 200, 26.7.2016, p. 1–136).

document-issuing authorities and promote its continued use; and

- swiftly implement the Regulation on promoting the free movement of citizens by simplifying the requirements for presenting certain public documents in the EU and exploit its potential to enhance public document security through use of the Internal Market Information system.

The Commission will:

- assess the current situation in Member States, and facilitate discussion on biometric identifiers (facial image and/or fingerprints) in population registers, in full respect of EU data protection law and taking account of the national context in Member States;
- facilitate discussion on how breeder documents can be made more secure, from the second quarter of 2017;
- work with key partner third countries to promote and support the introduction of biometric identifiers in their population registers;
- strengthen R&D activities in the area of breeder documents and document verification, including the evaluation of mobile technologies, in the framework of the Horizon 2020 programme for Secure Societies 2018-2020; and
- monitor implementation of the Regulation on promoting the free movement of citizens by simplifying the requirements for presenting certain public documents and assess its potential to further enhance electronic public document security.

2. Issuance of documents

At the Council meeting in December 2005, all EU Member States adopted conclusions [11] on minimum standards relating to the security of issuing processes for Member States' identity cards. This was followed up by a Resolution in 2006[12]. The recommendations address the issuance of ID cards to be used as travel documents, but they are relevant for all travel documents. Nevertheless, some (for instance, requiring applicants to apply in person and monitoring the whole issuing process) are still not fully implemented.

It is important that Member States exchange best practices as regards both biometrics enrolment and document granting and issuing procedures, in order to achieve greater coherence between national practices. The Commission will facilitate this by organising workshops and *ad hoc* meetings.

We know that decentralised issuance processes make it easier for fraudsters to steal and re-use blank documents. Centralising and monitoring/auditing issuing and personalisation processes (filling-in of blank documents) prevent the circulation of (in particular, blank) stolen documents.

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

[12] Resolution of the Representatives of the Governments of the Member States, meeting within the Council on 4-5 December 2006, on minimum security standards of identity cards valid for travel issued by Member States.

Specific actions
Member States should: - ensure full implementation of the 2006 Resolution on minimum standards as regards the security of issuing processes; - exchange information on best practices regarding biometrics enrolment and document granting and issuance procedures; and - strengthen the monitoring of the personalisation/issuance of identity and travel documents in order to limit the number of blank stolen items. *The Commission will:* - facilitate the exchange of best practices on issuing procedures and identity management by organising workshops from the first quarter of 2017.

3. Document production

3.1 Security features in travel documents

EU legislation has been adopted on standards for security features and biometrics in passports and travel documents issued by Member States[13] and on uniform formats for visas[14] and residence permits for non-EU nationals.[15] These standards are also used for local border permits[16] and permits issued in the framework of the legal migration *acquis*. The relevant technical specifications for documents are continuously updated to prevent fraud and it is thus important that documents are produced in full conformity with the latest versions of these technical specifications.

The Commission has presented two proposals[17] to upgrade security features and establish a new design for visa and residence permits for third country nationals. The rapid adoption of these proposals would help to reduce the use of forged documents to enter the area without controls at internal borders.

Currently, security levels of national ID cards delivered by Member States and of residence documents for EU nationals residing in another Member State and their family members vary significantly, which increases the risk of falsification and document fraud as well as leading to practical difficulties for citizens when they seek to exercise their right of free movement. As a follow up to the 2013 EU Citizenship Report and as noted in the Communication of 2016 "Enhancing security in a world of mobility", the Commission launched a study[18] to further assess security issues, including a possible harmonisation of security features to enhance their

[13] Regulation (EC) No 2252/2004 (OJ L 385, 29.12.2004, p. 1). UK and IE are not part of this measure.
[14] Regulation (EC) No 1683/95 (OJ L 164, 14.7.1995, p.1).
[15] Regulation (EC) No 1030/2002 (OJ L 157, 15.6.2002, p.1).
[16] Regulation (EC) No 1931/2006 (OJ L 405, 30.12.2006, p. 1).
[17] Proposal for a Regulation amending Regulation (EC) No 1683/1995 of 29 May 1995 laying down a uniform format for visas (COM(2015) 303 final); Proposal for a Regulation amending Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third country nationals (COM(2016) 434 final).
[18] Study to support the preparation of an impact assessment on EU policy initiatives on residence and identity documents to facilitate the exercise of the right of free movement.

resistance against document fraud risks. Enhancing the security features of ID and residence documents could also help address the problem noted in recent reports of the European Border and Coast Guard that national ID cards with a lower security level are the most frequently detected false documents.

In the context of the right to consular protection enjoyed by EU citizens whose Member States do not have diplomatic or consular representation in a third country, another Member State might need to issue Emergency Travel Documents to such citizens. A Decision from 1996[19] established a common format for such Emergency Travel Documents to enable the citizens to travel home. Issuing Emergency Travel Documents constitutes the most frequent type of consular assistance. After 20 years, this Decision is outdated[20]. Some Member States do not use the Emergency Travel Document due to the fact that it is considered unsecure against document fraud. In the context of this revision, the Commission will explore possibilities also to modernise security features of Emergency Travel Documents.

3.2. Enrolment of biometrics

EU-level guidelines have been adopted for authorities enrolling biometric identifiers in passports and residence permits for third country nationals[21]. This is a very important task, as most non-matches at border control are caused by the faulty enrolment of data at the time of issue. Biometric quality is the most important parameter affecting the accuracy of automatic biometric systems. Biometric vulnerabilities such as 'face-morphing' and 'fingerprint spoofing'[22] should also be addressed.

Specific actions
The European Parliament and the Council should: - adopt as soon as possible the proposals on a more secure uniform format for visas and residence permits for third country nationals to avoid further fraud. *The Commission will:* - in the first quarter of 2017, finalise the study on EU policy options to improve the security of EU citizens' ID cards and the residence documents of EU citizens residing in another Member State and of their non-EU family members in order to limit the risk of fraud and forgery. The Commission will evaluate the next steps, options and their impacts, in view of a possible legislative initiative by the end of 2017. - examine whether there is a need to amend Regulation (EC) No 1931/2006 to ensure that the conditions for issuing local border traffic permits, and the security features of the permits, guarantee appropriate security risk assessments while not prejudicing in any way the benefits of the Regulation and the Schengen Borders Code for the

[19] Decision of the representatives of the Governments of the Member States meeting within the Council of 25.06.1996; OJ L168 of 6.7.1996.

[20] Also due to the entry into force of Directive 2015/637/EU on the coordination and cooperation measures to facilitate consular protection for unrepresented citizens of the Union in third countries.

[21] Commission Decision C(2011) 5499 of 4 August 2011.

[22] Face-morphing: blending two facial images into one with the assistance of digital programmes; fingerprint-spoofing: use of fake fingerprints by copying fingerprints onto rubber.

permit holders.

- develop further guidance/training for the correct enrolment of biometric identifiers, in particular to address biometric data quality and vulnerabilities from the third quarter of 2017 and
- monitor the conformity of security features of travel documents issued by Member States against EU technical specifications.

4. Document control

The Schengen Borders Code[23] sets out procedures for checks on EU and non-EU nationals at the external borders. Border guards have to perform these checks quickly and rely on technologies/databases, training and guidance tools to enable them to verify travel documents.

4.1 Electronic checks on non-EU nationals' travel documents

The electronic verification of the authenticity of non-EU nationals' travel documents is an essential component of the future Entry/Exit System;[24] it contributes to security, as it helps to detect and combat identity fraud and the misuse of travel documents. In addition, the system will combat identity fraud by managing non-EU nationals' biometric identity, in much the same way as the Visa Information System does for visa-holders. The two systems are closely interconnected for these purposes.

Obtaining certificates from non-EU countries (country signing certification authorities) to authenticate the travel document is a time-consuming and sensitive process, but it is necessary to make sure that the chain of trust from the 'producer' of the certificate to the 'consumer' (user) is unbroken. The Commission started a pilot project in 2015 to explore how to collect non-EU country certificates, validate their trust level and subsequently share them in the form of a 'masterlist' complying with an International Civil Aviation Organisation specification.[25] As of 2017, this 'masterlist' could simplify and further promote the electronic authentication of non-EU country travel documents for all Member States.

4.2 Database checks

Document holders should immediately report the loss or theft of their documents. If Member States enter the information promptly in the Schengen Information System (SIS) and Interpol's stolen and lost travel document database, as they are legally required to do, it greatly reduces the chances of identity fraud. As of 24 November 2016, there were over 52 million SIS alerts on issued documents and 1 million for blank documents. In 2015, there were around 18 500 hits for issued documents.

Member States should also pass on to Interpol data on lost, stolen or misappropriated travel documents issued by non-EU countries so that it can enter the data into the stolen and lost

[23] Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 77, 23.3.2016, p. 1).

[24] COM(2016) 194 final, 6.4.2016.

[25] A masterlist combines the certificates of different country signing certification authorities and is published by one country which has verified the certificates and signed the list. The procedure is set out in ICAO document 9303.

travel document database where possible. This is particularly important in relation to fraudulently obtained Syrian travel documents, for example. The stolen and lost travel document database contains over 68 million records, which were searched over 1 243 billion times between January and September 2016, resulting in over 115 000 hits.

The proposed amendment of the Schengen Borders Code[26] would make it obligatory to verify all travel documents, regardless of the holder's nationality, against the SIS and the stolen and lost travel document database. This would make it easier to identify lost, stolen, misappropriated or invalidated documents and to seize them or preserve them as evidence. In addition, the proposed European travel information and authorisation system (ETIAS)[27] should make it possible to check visa-exempt non-EU nationals' travel documents against the SIS and the stolen and lost travel document database prior to their arrival at the external borders. The High-Level Expert Group on Information Systems and Interoperability[28] is looking at how interoperability could contribute to improved document and identity checks.

4.3 Training

Member States, competent EU agencies and the Organisation for Security and Cooperation in Europe (among others) have developed training for border guards on the detection of document fraud. This needs constant updating, notably to focus on new forms of fraud, such as look-alike fraud, and to address all those involved in verifying documents, such as carriers, consular staff and local administrations.

The Carriers Liability Directive provides for financial penalties for carriers who transport non-EU nationals lacking the necessary documents for entry to the EU. Further consideration should be given to including suitable provisions on training for carriers in order to improve the detection of document fraud.

4.4 Tools

Available tools to help police officers, border guards and others to detect document fraud include the false and authentic documents online database (FADO), which is a European image database with standardised descriptions, in the 24 official EU languages, of document security features and falsification techniques and several link option functions providing direct access to other document-related databases, as well as national and commercial applications.

FADO was set up in cooperation between Member States and should be brought within an EU legal framework. At present, Member States are under no legal obligation to upload documents (whether their own authentic ones or falsified ones they have detected) and this results in wide variation in the extent of contributions as regards both their own and non-EU country documents. In addition, actual use of the database is still limited. An analysis should be carried out on the added value of the system and on whether improvements are necessary.

---

[26] The proposal for an amendment to the Schengen Borders Code (COM(2015) 670 final, 15.12.2015) will be formally adopted in the first quarter of 2017.

[27] Proposal for a Regulation of the European Parliament and the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624 (COM(2016) 731 final).

[28] This was established following the Commission Communication on *Stronger and smarter information systems for borders and security* (COM(2016) 205 final, 6.4.2016).

Apart from the police and border authorities, civil and private entities[29] that need to perform identity checks for various reasons also rely on the use of genuine travel and identity documents. The 'non-document-expert' community should also be able to rely on simple authentication mechanisms that do not require expert knowledge or specialised equipment. Non-experts and the general public have access to a subsystem of FADO which provides less detailed information. Means should be explored of giving them wider access to lost or stolen document alerts, databases on genuine documents and recent alert information on fraud trends.

4.5 Biometrics in travel documents

Biometric identifiers are an important tool for detecting fraud. Border control officials can use them to establish identity, in particular by comparing the data on the chip with those on the document.

In order to check the electronic components of e-passports and e-residence permits, the authorities need the Member State that has issued the document to provide them with the requisite certificates so that they can access the fingerprints stored on the chip. The systematic electronic checking of the chip data would lead to the detection of the most common cases of document fraud, such as manipulations of the photo of the holder. Unfortunately, not all Member States exchange their certificates.

The SIS's potential to tackle document fraud will grow with the implementation of a 'fingerprint search' functionality. The first elements (the data-quality control mechanism) will be ready by mid-2017 and the work at central level will be completed in the fourth quarter of 2017. The functionality will enable the successful identification (via their fingerprints) of persons sought by the authorities. The automated fingerprint identification system (AFIS) will perform identity checks and contribute significantly to the detection of document and identity fraud. Member States will be phasing it in from the start of 2018.

Stolen, misappropriated, lost or invalidated passports, identity cards, driving licences, residence permits and travel documents can already be entered in SIS, but the Commission is envisaging proposing (as part of the revision of the system's legal basis) that falsified documents should also be entered. This will enable a more comprehensive approach to the detection and seizure of such documents.

[29] e.g. postal services, banks, notaries, travel agencies, car rental firms, money transfer agencies.

Specific actions
Member States should: - systematically register all stolen, lost, misappropriated or invalidated documents in the SIS and the stolen and lost travel document database to ensure that they are seized and/or preserved as evidence for criminal proceedings if presented again by the holder, thus effectively taking them out of circulation; - systematically feed Interpol databases with data on lost, stolen, misappropriated or invalidated travel documents issued by non-EU countries, where those countries do not do so themselves. - ensure that border guards have better access to the relevant information systems; - improve data collection and information exchange on document fraud, especially on look-alikes, fraudulently obtained genuine documents and identity fraud; and - accelerate the implementation of the fingerprint search functionality in the SIS. *The Commission will:* - propose that the legal basis of the SIS be revised so that Member States can enter falsified travel documents in the system in December 2016; - discuss with Member States how to improve the use of the false and authentic documents online database (FADO), including examining options for its future development, synergies and added value starting in the first quarter of 2017; - provide for a regularly updated list of certificates needed for the electronic authentication of travel documents during the third quarter of 2017; - work together with the competent EU agencies to boost training activities in new areas of document fraud; - explore the feasibility of including training requirements in the Carriers Liability Directive; - examine how to improve the availability of information on new and false documents to the 'non-document-expert' community during the fourth quarter of 2017; - continue to monitor the implementation of EU law on the use of biometric applications for document security and the exchange of certificates among Member States; and - implement a 'fingerprint search' functionality at central level in SIS in the fourth quarter of 2017.

III. FOLLOW-UP

The Commission calls on Member States to take all necessary steps to ensure the swift implementation of this action plan. It will report to the European Parliament and the Council by the end of the first quarter of 2018 on the progress achieved.