OSCE Organization for Security and Co-operation in Europe

OSCE ODIHR

COMPENDIUM OF GOOD PRACTICES IN IDENTITY MANAGEMENT IN THE OSCE REGION

COMPENDIUM OF GOOD PRACTICES IN IDENTITY MANAGEMENT IN THE OSCE REGION

OSCE Organization for Security and Co-operation in Europe

OSCE ODIHR

Published by the OSCE Office for Democratic Institutions and Human Rights (ODIHR)
Ul. Miodowa 10, 00-251 Warsaw, Poland
http://www.osce.org/odihr

ISBN 978-92-9234-954-7

Designed by Homework
Printed in Poland by Agencja KARO

TABLE OF CONTENTS

FOREWORD

The Organization for Security and Co-operation in Europe (OSCE) promotes the understanding that secure identification is not only about document security, and that processes for the legal establishment and registration of the identity of every person, as well as the management of these data, is an integral part of secure identification.

Secure and efficient systems for civil registration and identification, as well as residency registration, as components of identity management infrastructure indirectly, but decisively, determine to what extent people enjoy certain basic rights. Depending on the provisions in place, these systems can help to ensure that citizens can exercise a wide range of rights, such as those to property, privacy, freedom of movement and free choice of place of residence, as well as access to social services, including education, health care and social security.

Travel documents, in particular, provide for freedom of movement and cross-border movement, allowing the development of human contacts and relationships across the OSCE region and internationally. As the most important instrument for the facilitation of international travel, travel documents designed in line with relevant international standards to allow for fast and secure travellers' identification and facilitate their processing at the borders. However, the fact that the design of the document follows international standards is not enough to ensure it is secure. The document needs to be protected against counterfeiting and forgery and, crucially, needs to be issued on the basis of a verifiable identity.

Despite the fact that border controls are tightening and highly secure passports with biometric chips are now in wide use, the processes to obtain these passports vary from country to country and are often not as secure as we would like to think. The emerging trend in travel document fraud is that authentic documents are obtained on the basis of false identities, thereafter making them extremely difficult to detect at border crossings or within a state's territory. Therefore, robust identity management infrastructure that supports issuance of identification documents is essential as the OSCE region faces the challenges of preventing the movement of terrorists, combating organized crime, and managing irregular migration. For this reason, OSCE participating States have committed themselves on multiple occasions to establish effective controls on the issuance of national identity cards and travel documents, as well as to implement measures for ensuring the security of these and preventing their counterfeiting, forgery and fraudulent use.

The Compendium combines the perspectives of the OSCE Office for Democratic Institutions and Human Rights (ODIHR)'s work on identity management and freedom of movement, and the OSCE Transnational Threats Department's work on travel document security. It is the result of consultations initiated in 2013, and the subsequent process has included a series of expert meetings and a detailed questionnaire distributed to all OSCE participating States in August 2016.

This Compendium builds upon existing ODIHR expertise in civil registration, identification, and population registration and reform, as well as in providing technical support to participating States in this area. This publication can be seen as an expanded new edition of the ODIHR *Guidelines on Population Registration*, published in 2009, which will continue to guide participating States in improving their practices.

Breaking new ground in its holistic presentation of identity management, this Compendium bridges the different dimensions of security to provide insights and guidance on a complex area. We hope it will be used by states to compare and contrast their identity management systems with others, to identify possible security gaps or weak links in their own systems, and to remedy these gaps using some of the good practices highlighted.

We would like to express our gratitude to the many international identity management experts – over thirty – who contributed to the development of this Compendium, including experts from the International Civil Aviation Organization (ICAO) Implementation and Capacity Building Working Group (ICBWG), the International Organization for Migration, the UN Refugee Agency and the European Union.

Ingibjörg Sólrún Gísladóttir

Director of the OSCE Office for Democratic Institutions and Human Rights

Rasa Ostrauskaite

Co-ordinator of Activities to Address Transnational Threats, OSCE Secretariat

1. INTRODUCTION

As the world's largest regional security organization, with 57 participating States spanning five continents from Vancouver to Vladivostok, the OSCE is well-positioned to support global efforts to improve identity management processes. OSCE participating States have adopted a range of commitments aimed at facilitating freer and wider travel in the OSCE region, and improvements in the security of travel documents has a direct and positive effect on visa facilitation processes. In line with these dual mandates, the OSCE Executive Structures actively co-operate to support participating States in both the security of borders, and the facilitation of cross-border mobility.

In November 2013, in order to support the ICAO Traveller Identification Programme (TRIP), the OSCE organized an Expert Roundtable on Addressing the Link between Travel Document Security and Population Registration/Civil Registration Documents and Processes. It is worth repeating one of the primary recommendations that emerged from this roundtable:

"Given the diversity of civil registry systems in operation and national discrepancies in how well they are linked to travel document issuance, the OSCE should develop a compendium of best practices on effectively linking the most common civil registration systems in the OSCE region with travel document issuance systems. This compendium would allow OSCE participating States to compare their own system to best practice examples that are most similar to their own system thereby allowing them to spot potential weaknesses. Likewise, this compendium could be used for capacity-building purposes in the OSCE area."

Following United Nations Security Council Resolution (UNSCR) 2178, which expressed grave concern about those who attempt to travel to become foreign terrorist fighters, there is a major focus in preventing the cross-border movement of terrorists and terrorist groups. The OSCE Ministerial Council has responded by calling for efforts to prevent the movement of foreign terrorist fighters through effective border controls and controls on the issuance of identity papers and travel documents. This strengthened recommendations from the expert community to improve information sharing on good practices in identity management. Equally, effective identity management systems are essential for participating States to meet a number of human dimension commitments, and their effective operation allows citizens to exercise a wide range of rights, including rights to access state services such as education, to freedom of movement and free choice of place of residence.

Therefore, the OSCE initiated a consultative process involving joint work by its Warsaw-based unit working on population registration and freedom of movement as part of the Office for Democratic Institutions and Human Rights (ODIHR) and its Vienna-based unit working on travel document security. Coming at the problem from both the perspective of security, and of rights to human contacts across borders, these joint efforts agreed to develop a Compendium of Good Practices in Identity Management. Moving forward, the OSCE organized an expert group meeting in March 2016 to determine the content of a draft questionnaire to be sent to the relevant authorities of OSCE participating States. The experts also discussed other aspects of identity management systems which should be further researched and reflected in the Compendium, steps that included taking stock and reflecting on existing good practices. Following the circulation of the Questionnaire to OSCE participating States in August 2016, consultations were held in December 2016 and again in May 2017 in order to assess the results of the questionnaire and to prepare a first draft of the Compendium.

The development of the Compendium goes hand in hand with global initiatives that are led by ICAO and its ICBWG to promote evidence of identity as part of the ICAO Traveller Identification Programme. The European Union is implementing a related "Action Plan to strengthen the European response to travel document fraud", which incorporates issues related to identity registration and document issuance. The OSCE is working with these organizations, as well as with organizations participating in the Global Civil Registration and Vital Statistics Group, to explore how the Compendium can be further disseminated and identify opportunities for it to contribute to capacity building.

1.1. GOALS OF THE COMPENDIUM

In recent decades, many states' identity management systems have undergone tremendous changes that have mainly been driven by the computerization and digitization of public administration, resulting in a dramatic shift in terms of how personal information and other data are processed and retained. Paper-based processing and storage has gradually been replaced by digital processing and retention of data. Furthermore, even established systems for digital data processing are constantly being revisited and upgraded to benefit from improvements resulting from rapid advancements in information technology (IT). Improved IT solutions also present new opportunities for introducing more efficient and innovative ways to share information, as well as innovative solutions for improving the integrity and security of systems employed for the processing and sharing of data.

Contemporary identity management infrastructure is therefore constantly being improved with the aim of exploiting opportunities arising from rapidly advancing information technologies. These changes can be seen not only in the introduction of more advanced IT solutions, but the introduction of such solutions is often coupled with gradual, and in some cases dramatic, changes in the way that different national identity management actors process and share personal data.

The Compendium is intended for the use of identity management practitioners and policymakers who are exploring options to improve their national identity management infrastructure as a whole or some of its individual components. The benefit of the Compendium comes from the wealth of information it provides in a structured and analytical format about the characteristics of identity management systems in OSCE participating States.

The Compendium has several objectives:

- **Sharing the latest trends in the OSCE region when it comes to the way participating States approach identity management**: obviously, a certain body of knowledge already exists; however, identity management is a dynamic area, as countries develop and respond to new threats and challenges, making it vital to keep information up to date;
- **Identifying new trends and challenges**: as mentioned, countries are developing their systems for identity management and are coming up with new solutions. In this context, it is important to analyse existing trends and discuss the gaps and inconsistencies that exist among various regions or countries. A special focus is placed on digitization, which allows for faster data processing and more efficient verification. At the same time, there is a growing need to ensure that personal data is properly protected;
- **Mapping available models of identity management**: nowadays, there are many countries that have successfully implemented various models of identity management. While there is no one universal model that is applicable to every country, it is important to discuss some of the best practices and identify the pros and cons of each of them; and
- **Putting a particular focus on the prevention of identity fraud**: identity fraud is the main threat to the integrity of the entire identity management framework. The more a system is exposed to fraud, the less overall trust the public will have in the process, including its international dimension: in the context of increasing global mobility, a well-functioning national identity management system is no longer sufficient for preventing identity fraud; instead, a global or at the very least a regional approach is necessary.

1.2. HOW TO USE THE COMPENDIUM

The different approaches to identity management and the good practices described in the Compendium will allow users to identify differences and explore similarities with their own national systems. In the latter case, the Compendium could be used to suggest good practices that could be replicated in a particular national context.

Such good practices may be related to how specific vital life events are registered or practices related to determining who is entitled to a specific identification document. Since the Compendium also provides an overview of how different institutions responsible for various components of identity management co-operate and share personal data, this information can be used to inform national identity management reform processes by exploring the experiences of other countries.

The Compendium is also designed to be a living document that can be periodically updated to reflect changes in national identity management systems. As such, it can be used to provide reference background information to support regional discussions on good practices in identity management.

The information presented in the Compendium focuses on the two components of national identity management infrastructure common to all OSCE participating States: civil registration and civil identification. These two systems are operated for the purpose of establishing the legal identity of natural persons and providing **primary identity documents**.

While there are several layers of identity management that produce different types of identity documents, frameworks for issuing primary identity documents are the critical components of the entire identity management system. They provide a framework for the legal establishment of one's identity and identity documents on the basis of which other types of identity documents may be issued.

In elaborating on both components, the Compendium promotes greater links and synergies between civil registration and civil identification that are often seen as two seemingly separate processes.

In this context, the Compendium provides information on critical aspects of identity management systems and how they compare across the OSCE area based on:

- **Authorities in charge**: various ministries play a role in identity management; however, most countries treat this as a function of the Ministry of Justice or the Ministry of Interior;
- **Level of decentralization**: some countries have decentralized their systems of identity management, assigning the task to local or regional governments, while others have central governing bodies in charge;
- **Level of digitization**: there are major differences in terms of migration from paper-based to electronic record-keeping;
- **Primary means of identification**: some countries use unique personal identification numbers (PINs) for easier identification, while others do not employ a unique identifier and rely on other personal characteristics instead;
- **The use of data**: some countries use population registries almost solely for the purposes of issuing corresponding services (identification documents, passports, etc.), while in other countries identification services may be rendered electronically by public or private third parties;
- **Data verification**: the number of checks to be conducted before a decision is made on the issuance of a document is another factor that varies dramatically from country to country;
- **Decision-making**: there is a great variety in terms of the number of individuals and/or instances within the relevant authority involved in the decision-making process; and
- **Interoperability/Interconnection**: in any country there can be a wide range of agencies being part of identity management infrastructure. Their systems for data sharing rely on interconnections between their data management systems with various degrees of interoperability between these systems.

While these are just a few examples, it should be noted that some differences are a matter of administrative tradition, while others can play a crucial role in the level of a system's security and trustworthiness.

1.3. STRUCTURE AND CONTENT

The Compendium is structured into four main sections: I. Dimensions and Components of Identity Management, II. Civil Registration, III. Civil Identification and IV. Risk Analysis.

The first section outlines the key human and security **dimensions of identity management**, and then the main **components** of identity management systems.

The section on **civil registration** elaborates on the benefits and value of civil registration, while also categorizing the civil registration systems employed by OSCE participating States according to the responsible administrative authorities, the administrative arrangements for civil registration and the procedures for civil registration. In terms of civil registration, the Compendium looks primarily at birth registration, highlighting its overall value for the legal recognition of an individual's identity and the subsequent issuance of identification documents. Furthermore, the Compendium elaborates, in a structured format, on the different approaches taken by OSCE participating States when it comes to the processing and retention of civil registration data and highlights trends and good practices.

The section on **civil identification** discusses the issuance of official identity documents, as these are the kinds of identification documents most frequently issued by most OSCE participating States either as mandatory documents or upon request. In addition to national identity cards, the section also covers the issuance of travel documents issued upon request by all OSCE participating States. The section describes the characteristics of civil identification systems, i.e., the authorities in charge, the administrative arrangements for the processing and storage of information and, finally, the procedures for application and the decision-making process of granting identification documents or renewing an existing document. The section describes three different approaches to the issuance of identification documents used by participating States and provides good practices specific to each of these approaches.

The Compendium focuses primarily on how participating States register and manage the identity of citizens on their territory. In addition, the Compendium also provides information on the processing of the identity information of resident non-citizens with permanent-resident status on a state's territory. The practices elaborated in the Compendium are, however, not applicable in the cases of other categories of foreigners who can be found on a state's territory, such as irregular migrants, asylum seekers and refugees. This is primarily due to various complexities related to the identity management of these categories of foreigners.

The final section on **risk analysis** reviews fraud and options for prevention. Important products of every identity system are the certificates serving as a proof that a certain vital life event has taken place and documents used for identification, whether within the state in the form of national identity cards or internationally in the format of travel documents. From the perspective of identity management, it is very important that these documents are secure and cannot be recreated or fabricated by unauthorized persons and/or organizations. The moment this is not the case, the credibility of the entire identity management chain can be tarnished and seriously questioned. Therefore, protection of the document against fabrication and forgery has become very important and it has become imperative that each new generation of issued identification documents is enabled with new and innovative security features.

The protection and production of secure travel documents, although important, is not covered by the Compendium. Instead, the main emphasis is placed on the process that leads to determining the right identity information and physical identifiers which are then subsequently used for the personalization of secure identification documents.

1.4. METHODOLOGY, DATA GATHERING AND ANALYSIS

The information presented in this Compendium is the result of research and statistical analysis conducted in the period from March 2016 to May 2017. The information used for the analysis conducted for this study was obtained mainly through a questionnaire developed for this purpose by ODIHR and distributed to the relevant authorities in all 57 OSCE participating States. The design of the questionnaire was determined during a preparatory meeting organized by ODIHR in partnership with the OSCE Secretariat's Transnational Threats Department in March 2016 in Warsaw.

The questionnaire comprised a range of questions covering matters such as: the characteristics of each state's civil registration system, information on the issuance of official identity documents and travel documents, application procedures for an identification document, verification of identity information for citizens and resident non-citizens, and the type of personal information collected, processed and stored in official databases.

The questionnaire thus formed the basis for a comparative analysis of different OSCE participating States in terms of their administrative arrangements for the collection, processing and retention of personal information as part of civil registration and civil identification, as well as a comparative analysis in terms of procedures for the registration of vital life events and determination of who is entitled to an official identity document and/or travel document. The blank questionnaire forwarded to OSCE participating States is included as Annex 4. The information obtained from the questionnaires was also used to conduct statistical analysis of the implementation of specific tools in identity management (e.g., verification of data contained in submitted documentary evidence).

The questionnaire was distributed to the national authorities of all 57 OSCE participating States, and 41 of them provided the OSCE with a completed questionnaire. The following OSCE participating States provided their responses: Albania, Andorra, Armenia, Austria, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Canada, Croatia, Cyprus, Estonia, former Yugoslav Republic of Macedonia, Georgia, Greece, Hungary, Ireland, Italy, Kazakhstan, Kyrgyzstan, Latvia, Liechtenstein, Lithuania, Luxemburg, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom and United States of America.

Where information was not obtained via the questionnaire, the analysis was supplemented by information publicly available on the official websites of the relevant government authorities.

Further to the information obtained via returned questionnaires, the analysis benefited from global analyses of identity and civil registration systems aggregated in the "Identification for Development Global Dataset" compiled and published by the World Bank.[1]

Comparative analysis was used to assess how different states have approached the administrative setup for civil registration and civil identification, the authorities in charge and how and to what extent different national stakeholders co-operate to form a unified identity management infrastructure. The analysis was also used to examine and compare different states' approaches to application procedures for identification documents and the criteria for determining who is entitled to an identification document.

Statistical analysis was used to analyse all the responses to a series of yes-or-no questions, so as to determine to what extent specific features of identity management and the tools for its management are being implemented across the OSCE. The statistical results are provided in terms of the total number of questionnaires where the authorities provided responses to the questions. The results also show how many states did not respond to a question.

The quality and accuracy of the information provided by participating States' national authorities is not fully guaranteed nor was it further verified thorough in-person interviews. To some extent, the information may not be completely accurate, as responses depended on an understanding of the questions by the officials who completed the questionnaire. In some cases, an answer was not provided because the officials might not have been familiar with the information that was requested. Although there may be a margin of error in terms of the responses used in the statistical analysis, the final result of the analysis can be read as an important indicator of trends when it comes to specific identity management practices in the OSCE region.

1 Identification for Development Global Dataset (Washington: The World Bank, 2016), < http://data.worldbank.org/data-catalog/id4d-dataset>

2. DIMENSIONS AND COMPONENTS OF IDENTITY MANAGEMENT

2.1. THE HUMAN DIMENSION OF IDENTITY MANAGEMENT

Each country's identity management system also provides a framework for observing and protecting many of the human rights embodied in international declarations and conventions. Depending on the provisions in place, the system can ensure that citizens can exercise a wide range of rights, such as rights to property, privacy, freedom of movement and free choice of place of residence, as well as access to social services such as education, healthcare and social security. In some states with more advanced technological infrastructure, population registration provides the basis for the establishment of a number of citizen-oriented computerized services, also known as e-services and e-government. Identity management is also central to prevention of discrimination in exercising guaranteed rights. Exclusion from the civil register can, for example, put people at risk of statelessness and exclude vulnerable communities such as Roma and Sinti from services.

The identity management infrastructure provides the backbone for a functioning and viable state by securing civil, population and tax registers, as well other systems such as healthcare benefits, voter lists and the issuance of travel and identity documents based on verifiable identities. These steps strengthen the rule of law and foster democratic governance.

The incorrect attribution of an identity and flaws in an identity management system have the potential to disrupt the effectiveness of government activities. Such flaws may become visible during elections, where shortcomings in voter lists can affect confidence in the election process. Flawed identity management systems can also result in unintended discrimination when it comes to enabling access to various rights and state-guaranteed services. A system that is vulnerable to abuse may allow for the creation of multiple identities, registering for services in more than one location or identity theft, which can severely undermine state credibility. Such abuses can ultimately result in a negative public or political perception and/or awareness that many individuals are not receiving the services to which they are entitled or that some individuals are receiving services to which they are not entitled.

In essence, a secure identity management system can be seen as the foundation, a root level,that is able to then feed into and help numerous other branches of key state services function effectively and accurately.

2.2. THE SECURITY DIMENSION OF IDENTITY MANAGEMENT

Similarly, one of the key elements of a secure environment for cross-border travel is that the travel documents used by visitors meet international standards in terms of security of the document itself and security in that the document must reflect the genuine identity of its holder. Where there is a lack of trust in the security of travel documents issued by another country and a lack of confidence in the procedures used for issuing these travel documents, states generally choose to introduce barriers to the freedom of movement.

Identity and travel documents can only be as secure as the documents feeding the system that issues them. While elaborate international standards have been developed to support the introduction of secure machine-readable travel and identification documents, to date no international standards exist for these so-called breeder documents used to validate an identity. As the international organization that sets the standards for travel and identity documents, the International Civil Aviation Organization (ICAO) responded to this need by adopting its global Traveller Identification Programme (TRIP) Strategy. The first component of the TRIP Strategy, titled "Evidence of Identity", specifically targets the security and quality of travel documents at the stages of application and issuance, aiming to ensure that these documents are not only secure but also based on genuine and verifiable identities and with numerous government services relying heavily on accurate identity information, investments in improving such systems have multiple positive impacts. A detailed overview of the ICAO TRIP strategy and related guidance materials is elaborated in Annex 3 of this document.

Establishing better practices for national identity management can include a range of measures, including strengthening proof of identity, such as birth certificates, civil registry entries and other methods used to verify and/or validate a document applicant's identity. Similarly, the systems for issuing travel documents need to be linked to identity management systems to streamline decision-making processes, preferably through modernized systems that reflect developments in document technology.

As entries in registers or officially issued identification documents provide access to specific services, criminal networks are constantly looking for possible gaps in identity management systems to obtain genuine documents under fabricated or stolen identities. Documents obtained as result of gaps in identity management have enabled criminals to target business entities and cause significant financial losses through the use of genuine documents issued to non-existent identities.

2.3. IDENTITY MANAGEMENT AND ITS COMPONENTS

The right to an identity is a fundamental right that enables individuals to be recognized in their interaction with the state and in legal transactions with other individuals and legal entities. Without an identity recognized by states, a person may not have access to or may face obstacles in accessing many fundamental rights and state services, such as healthcare, vaccination programmes, education, social protection, a bank account or birth, identity or travel documents.

The right to an identity was established in Article 6 of the Universal Declaration of Human Rights of 10 December 1948: "Everyone has the right to recognition everywhere as a person before the law."

The starting point in the creation and managing of a person's official identity is their registration by the appointed governmental institution. It is the government's responsibility to decide which framework to employ for identity recognition. In all states in the OSCE region, civil

registration is the basic method. An individual's identity is established through birth registration, which provides evidence of their identity in a form of certificate that is then used as a breeder document for all other identification documents subsequently issued.

Apart from a civil registration certificate, which does not usually include information that links identity data with the document holder, many governments issue either mandatory or optional civil identification documents. These civil identification documents provide not only certified information about an individual's identity but also information about their physical appearance in order to ensure proper identification.

Citizens' ability to exercise their rights in their interaction with the state and to enter into legal transactions with other individuals and legal entities relies on the state's ability to properly register vital life events, register and protect personal identity information, and ultimately provide a secure framework for the identification of individuals. In practice, this has resulted in the creation of a comprehensive legal and administrative system for identity management. In some cases, the identification system functions as a single entity; however, it is more often the case that an identity management system will comprise different government actors with their own systems for processing personal information that work together to maintain the integrity and credibility of the national infrastructure for identity management.

All organizations that deal with a large number of individuals in order to regulate access or entitlements to specific services use some form of management of identity information to determine individuals' rights and privileges. The processing of identity information to determine people's entitlement to specific services can occur between individuals and the state, as well as in interactions between individuals and other legal entities that provide paid services.

Broadly speaking, identity management can be defined as a combination of specified systems, rules and procedures used between an individual and organizations regarding the entitlement, use and protection of personal information in order to authenticate individual identities and **provide authorization and privileges** within or across systems and enterprise boundaries.

Authentication of individual identities is achieved through the issuance of identity documents. These documents are used for the purpose of verifying an individual's identity or as a means of identification when applying for entitlements granted to that specific identity.

Identity management takes place on three different levels (Figure 2.1), each providing identity documents of a different value. They can be broadly categorized as follows: – primary identity documents issued for the purpose of establishing an individual's legal identity; – secondary identity documents that enable access to certain rights and privileges and are issued only on the basis of the presentation of a primary identity document; and – tertiary identity documents that enable specific entitlements.

FIGURE 2.1 THREE CATEGORIES OF IDENTITY DOCUMENTS

Primary Identity Document (PID) *(Establishes legal identity)*	**Secondary Identity Document (based on PIDs)** *(Rights and privileges)*	**Tertiary Identity Document** *(Entitlements)*
Certificate(s) issued by the civil register	Voter card	Social security card
Identification document issued by the Civil Identification Agency	Divers license	Health service card
	Student ID	Membership card
	Passport	Employee badge
	Bank (account) card	Conference badge

The value of an identity management system can be found in the fact that it enables state authorities to establish an individual's legally recognized identity, issue other identity documents for identification purposes and manage access to various entitlements on the basis of recorded identity information.

Civil registration and civil identification systems, including the corresponding legislative framework and administrative arrangements, are under national sovereignty. This means that each state has the exclusive right or competence to determine the character of its institutions, to enact laws of its choice and to ensure their respect. Furthermore, states also have exclusive authority to exercise their authority over all persons and things found within their territory. However, there are instances in which states have accepted to be bound to specific international standards. An example of such an approach is the broad acceptance of standards set forth by the ICAO in relation to the design of travel documents and national identity cards designed to also be used as travel documents.

In the EU context, national sovereign authority over the design of identification documents has been also delegated to the EU authorities who set the EU-wide standards for the design of EU residence permits and travel documents issued by Member States.

An identity management system comprises the following key elements:

A natural person: a unique human being who, from birth, has a biometric identity that is based on their appearance, as well as physical and behavioural characteristics (e.g., gait, voice-recognition);

Identity: a unique set of features and characteristics that individualize a person, including their name and other biographical data;

Legislation, regulations and procedures: developed on the basis of international conventions and national culture, administrative tradition and customs uniformly implemented by civil registration and civil identification authorities;

Identity management systems: need to be implemented in an effective and efficient way to be able to support automated registration of newborns or foreigners residing in a country, so that reliable proof of identity can be provided when necessary throughout a person's entire life;

Identity documents: are issued on the basis of the registration of a newborn or a foreigner residing in a country. Identity documents include birth, marriage and death certificates, as well as national identity cards and/or travel documents or any other documents that prove that an individual has been registered in a particular functional register; and

Managing identities and documents: registration or issuing authorities have an obligation, once a person's identity is established and registered, to manage their identity and the documents derived from that registration throughout their lifetime until death.

An important challenge for identity management authorities is keeping identity information up to date and maintaining the link between a person and their recorded identity.

One of the most important linkages in the public sector is that between the civil register and the civil identification register. This link is streamlined by turning the two systems into the main components of a national identity management system. Civil registration involves the recording of biographical information that also confirms one's "belonging", whereas civil identification involves the addition of certain attributes that ensure a unique, secure and legal identity. These attributes can be a unique personal number, photograph, signature, biometric data or citizenship confirmation, to mention just a few.

A basic condition for people to enjoy access to benefits and rights is that their existence is formally recognized through the process of civil registration and registration of vital life events, or more precisely, through birth registration and the issuance of a birth certificate that confirms their identity.

Birth registration is the first step towards establishing an individual's legal identity. Legal identity is not synonymous with citizenship, and for operational purposes it can be defined as the "legal civil status obtained through civil registration at birth and civil identification of unique attributes such as a personal identification number and biometrics that recognizes the individual as a subject of law and protection of the state."[2]

The United Nations Statistics Division (UNSD, 1998) defines civil registration as the continuous, permanent, compulsory and universal recording of the occurrence and characteristics of vital events (live births, deaths, foetal deaths, marriages and divorces) and other civil status events pertaining to the population as provided by decree, law or regulation, in accordance with the legal requirements in each country.

The institutional and administrative functions of the civil register are outlined in each country's national legal framework and are designed to reach and cover the entire population. The national approach to civil registration as the main provider of proof of identity is described in greater detail in the civil registration section of this Compendium.

Having a registered identity is not sufficient as long as there is no structure that can link identity information to a particular individual. Secure identity documents enable access to certain entitlements and rights for individuals based on identity information while making sure that the person in question is indeed the rightful owner of that identity. Furthermore, they ensure that entitlements are not provided to the wrong person, who might be interested in gaining access to someone else's identity by finding gaps in both civil registration and civil identification systems.

2 Dictionary for Civil Registration and Identification (Washington: Inter-American Development Bank, 2013), < https://publications.iadb.org/handle/11319/3679 >.

3. CIVIL REGISTRATION

A civil registration system records the occurrence of certain events such as births, deaths, marriages and civil partnerships, divorces, annulments, separations, parental relations and adoptions, changes in name or legal capacity in accordance with each country's legal requirements. These events are associated with an individual from birth to death, including all changes in civil status that may occur throughout an individual's lifetime. Some of these changes in civil status, such as birth and death (and, to a degree, parenthood and family descent), are natural events, while others are social events. What they all have in common is that there are laws that require that specifically these events (as opposed to other events) be recorded and registered in registers for administrative and other legal purposes in order to enable citizens to provide and be in possession of evidence of their social status. Nevertheless, there is a certain set of occurrences that are commonly defined as changes to "civil status" that has developed historically.

The United Nations defines civil status registration as the continuous, permanent, compulsory and universal recording of the occurrence and characteristics of vital events pertaining to the population as provided through decree or regulation in accordance with a particular country's legal requirements. Civil status registration is carried out primarily for the purpose of establishing the legal documents provided by the law.

All OSCE participating States have systems for registering births, marriages and deaths, as it is recognized that the accurate and comprehensive recording of key life events is essential to the state. Civil status registration records create a basic, continuous source of information about a country's population. Apart from providing a record of vital events in relation to the people living in a state, these records also satisfy the need for evidence of identity and civil status, which has a bearing on rights, entitlements, liabilities, status and nationality.

The civil register operating under the auspices of a government institution or a ministry is the sole and principal authority for the recording of vital events, such as births, adoptions, recognitions, marriages, divorces and deaths. It establishes a person's identity and "belongingness" through the issuance of certificates or legal documents that confirm and recognize their identity and legal situation before the state, society and their family.

As the need for a unique, verifiable form of identification grows, there is increasing recognition of the important role of the civil register as the custodian and anchor point of a person's unique, secure and legal identity.

Based on the information in their records, the civil register issues legal documents as described by law as proof of identity. These documents enable a person to access services and take advantage of a series of benefits, as well as their human, civic, political and financial rights.

The civil register is also an essential source of vital statistics. International organizations have promoted this aspect of civil registration to improve the completeness, quality and timeliness of reporting of vital statistics through civil registration and vital statistics initiatives. Improved vital statistics are important for informed decision-making and planning of public policies and programmes.

Furthermore, the civil register is the underpinning of a person's civil identification record and for the issuance of other national identification documents such as an identification card, passport and voter card. Civil identification involves the addition of attributes that uniquely and securely authenticate a person's identity. Such attributes include at least, but are not limited to, a unique personal number (assigned), the person's photograph, signature (dynamic), biometrics (inherent) or any combination of these elements.

The legal procedure required for registration is regulated by relevant legislation that prescribes a detailed legal procedure for registration of different types of vital life events (the procedure itself is not the subject of this Compendium). From the point of view of identity management, the Compendium looks at how civil registration records are created, processed and maintained and the verification of identities of individuals requesting the registration of vital life events, including administrative arrangements that ensure the legality of the process.

Legislation that guides civil registration at the national level generally follows the guidance of the United Nations Statistics Division. A detailed overview of UNSD guidance materials is available in Annex 3.

3.1. BIRTH REGISTRATION

Birth registration is essential for ensuring access to services such as healthcare, education and social services. It is a permanent and official recording of a child's existence and is a requisite part of civil registration.

It is important to highlight that, in most countries, birth registration, as part of civil registration, is the only legally recognized framework that provides citizens with the most important breeder document (certificate) that is subsequently used to establish their identity and to enable them to have their identity recognized in their interaction with the state and private entities. On the basis of their legal identity, a person can be provided protection by the legal system and can request that state institutions protect their rights. A person's legal identity can be proven by the presentation of official documents issued by the government, including documents certifying their age or civil status. Without such verification, a person may find it difficult to protect their rights (subject to their status) or to receive certain benefits.

Identity data collected and retained in civil registers provides the most important proof of identity in the process of issuing official identity documents such as an identity card or travel document linking identity information with a natural person.

The civil register is also important for states' ability to enable their citizens to access services and enjoy many civil rights. Information obtained from civil registers is essential to planning healthcare and education services, as well as urban planning, which have a direct impact on citizens' well-being.

When a child's birth is registered, he or she is issued a birth certificate. A birth certificate is a legal document that can ensure access to essential services such as healthcare, welfare grants or education. Later in life, this is necessary for tracking a child's age and to determine whether legal preconditions have been met to exercise the right to work and to get married. A child's ability to prove their age can ensure judicial protection and reduce the risk of being prosecuted as adults if they are underage and accused of a crime. In adulthood, birth certificates may be required to obtain social assistance, open a bank account, buy or prove the right to inherit property, vote and obtain a passport.

Birth registration also provides important evidence in the context of conferring citizenship and, under specific circumstances, preventing statelessness. The registration of births and acquisition of citizenship are distinct processes; however, birth registration serves as important proof of facts that form the basis for the conferral of citizenship. Birth registration may also be vital for confirmation of an individual's citizenship following tumultuous events such as armed conflict and situations of state succession.

3.1.1. The registration process

The objective of any civil registration procedure, including birth registration, is to issue a legal document that can be used as proof of identity. Different countries have different deadlines for enrolment in the civil register after a birth has taken place, ranging from 3 to 60 days. Countries that have linked their healthcare system with the civil register can carry out the notification immediately after birth and issue a birth certificate automatically.

The civil register contains an individual's biographical data: name, date of birth, place of birth, sex, name of parents and identifying information, such as the number of their identification documents, e.g., identity cards. The record may or may not include information on citizenship. Some countries note a person's religion and ethnicity in their records.

FIGURE 3.1 THE BIRTH REGISTRATION PROCESS

- This is an administrative procedure, and it is usually carried out by the health authorities if the birth takes place in a hospital or health centre.
- Parents or relatives may also notify the civil registry about the birth.

- This is a legal procedure.
- The creation of the individual's record is usually done by an official authorized to register vital events.
- The registration is requested by the child's mother, father or legal guardian. The person will have to show proof of identity.

- Once the content and all relevant and supporting documentation has been verified, a birth cerificate is issued.
- This is normally free of charge, but subsequent copies may carry a cost.
- The birth certificate is a legal document.

- The records that establish the identity will (ideally) be linked to the registration of all other vital events.
- The civil register record may also be the breeder record for civil identification.

The enrolment process generally requires presentation of a notification of an event and verification of proof of identity of the individuals submitting the application.

What needs to be ensured is that the vital life event indeed occurred (official notification), that the identity of the individuals requesting registration of the event is verified based on valid documentary evidence and that the vital life event is registered only once.

Notification is usually provided by informing organizations designated under the law for the registration of certain types of vital life events. For instance, for birth and death registrations these are normally healthcare providers, and a notification is normally sent to the relevant registrars *ex officio* by post or as an electronic notification. These notifications also contain, in case of birth, identity information about both parents or about the mother only in case information about the father is not known.

The registrar completes the registration process by creating a legal act of birth registration that contains all known information about the parents and the identity data attributed to the newborn. **As part of the registration process, the parents' identity data is verified, and it needs to match the identity information provided on the notification form**.

In Canada, birth registration is a two-step process. Two forms must be submitted and matched in order for a birth registration to occur. The first form, the Notice of Live Birth, is completed by medical staff and submitted to the relevant authorities of the province in question. The second form, the Statement of Live Birth, is completed by the parents of newborns using either a paper form or the Newborn Registration Service online and is then submitted directly to the Office of the Registrar General. It is the matching of these two forms that creates a birth registration.

In Kyrgyzstan, birth registration, as well as the registration of other types of vital life event, is under the authority of the State Registration Service.

Birth registration is initiated upon receipt of notification from the health authorities that a live birth has taken place. The information communicated by the health authorities also contains basic information on the identity of the person giving birth. The health authorities provide such notifications also in cases when the birth has taken place at home. A parent coming to register the birth of their child identifies herself/himself with a valid identification document (e.g. a national identity card). Registration officials must ensure that the identity information on the provided identity document matches the identity information recorded on the notification from the health authorities. Only then can the act of registration of birth be produced. One copy of the registration act is kept at the local branch of the Department of Population Registration and Acts of Civil Status while a second copy is transferred to the state archive of birth registration acts. Upon completing the registration, authorities also issue a birth certificate which the recipient may use when becoming eligible to obtain other identification documents.

In many OSCE participating States, citizens do not need to visit a civil registry office to complete a birth or death registration. In the United States, for example, all information required for registration of a birth is collected by the employees at the hospital where the birth takes place and is forwarded to the relevant state Vital Records Department. Verification of the identity of the mother or of both parents is carried out by the hospital staff.

When it comes to verification of the identity of the mother or of both parents, the practice across the region differs. In most OSCE participating states, registration is completed by the designated civil registration authority, but the registration process is either initiated only upon application by the mother or both parents or is carried out automatically based on a notification from the hospital where the birth takes place.

As parental information forms part of a newborn's identity data, it is important that the identity of the mother or of both parents be verified in the process. Here, practices differ, such as in the case of the United States and Georgia, where the identity of the mother or of both parents is determined by hospital staff upon admission, whereas in those states that require registration at the relevant registry office, the identity of the mother or of both parents is verified by registration officials.

In most OSCE participating States, to verify the identity data of the mother or of both parents, a hospital or the civil registration authorities require presentation of a national identity card or passport. In countries that do not issue national identity cards, other means of proof of identity can be accepted.

In most OSCE participating States, civil registration authorities request that individuals registering a specific life event present a national identity card in order to identify themselves and for verification of their identity data. Other official identity documents may also be accepted depending on the national regulations.

Identity cards not only provide legally valid identity information but also contain biometric information (a photograph and fingerprint in some cases), which enables easy verification of the link between the presented identity and a particular person.

Identity cards issued in the OSCE region are normally highly secure documents issued through a secure procedure. An electronic chip on the card adds another layer of security in case of any doubt about the security of the document.

In some OSCE participating States, additional verification can be carried out using online access directly to a database of issued identity cards to ensure that the presented document is genuine.

Two-step processes in birth registration (hospital notification coupled with a request for birth registration where applicable) are important for ensuring the integrity of the civil registration system. In reality, this means that only births that actually did occur are registered and linked with the identity of the mother as identified by the health authorities. Also, this further ensures that, for each notification, there can be only one registration and that if multiple registrations do take place for whatever reason, both registrations would point to the same identity. Any attempt to create a fabricated identity could be revealed by identifying a mismatch between the information in the registration request and the medical institution notification and in the mismatch between the number of notifications issued by hospitals and the number of births registered.

3.2. CIVIL REGISTRATION COVERAGE IN THE OSCE REGION

According to data gathered by the World Bank, civil registration coverage in the OSCE region is universal. Table 3.1 shows that according to these data, only in few participating States there is still a small percentage of the population that remains not covered. Where certain gaps exist, the data further reveals a fairly even gender balance in terms of the covered population. Where misbalance exists, it is generally extremely low.

TABLE 3.1 CIVIL REGISTRATION COVERAGE IN THE OSCE REGION (GENDER DESEGREGATED)

Country	Birth Reg. %	BR Males %	BR Females %	BR Gender Discrepancy	Reference Year	Country	Birth Reg. %	BR Males %	BR Females %	BR Gender Discrepancy	Reference Year
Tajikistan	88.4	89	87.8	-1.2	2012	Czech Republic	100	100	100	0	2012
Croatia	90	90	90	0	2011	Denmark	100	100	100	0	2011
Romania	90	90	90	0	2013	Estonia	100	100	100	0	2011
Azerbaijan	93.6	93.4	93.9	0.5	2006	Finland	100	100	100	0	2011
Turkmenistan	95.5	95.2	95.8	0.6	2006	France	100	100	100	0	2011
Kyrgyz Republic	97.7	97.6	97.9	0.3	2014	Germany	100	100	100	0	2011
Albania	98.6	99.4	97.9	-1.5	2008–2009	Greece	100	100	100	0	2010
Turkey	98.8	98.6	99	0.4	2013	Iceland	100	100	100	0	2010
Mongolia	99.3	98.8	99.2	0.4	2013	Ireland	100	100	100	0	2010
Montenegro	99.4	99.6	99.1	-0.5	2013	Italy	100	100	100	0	2011
Serbia	99.4	99.2	99.6	0.4	2014	Latvia	100	100	100	0	2011
Bosnia and Herzegovina	99.5	99.7	99.4	-0.3	2006	Lithuania	100	100	100	0	2011
Armenia	99.6	100	99.1	-0.9	2010	Luxembourg	100	100	100	0	2010
Georgia	99.6	99.4	99.9	0.5	2013	Netherlands	100	100	100	0	2011
Moldova	99.6	99.2	99.9	0.7	2012	Norway	100	100	100	0	2011
Kazakhstan	99.7	99.8	99.7	-0.1	2010–2011	Poland	100	100	100	0	2011
Former Yugoslav Republic of Macedonia	99.7	99.9	99.6	-0.3	2011	Portugal	100	100	100	0	2011
Ukraine	99.8	99.9	99.7	-0.2	2012	Russian Federation	100	100	100	0	2010
Uzbekistan	99.9	99.9	100	0.1	2006	Slovakia	100	100	100	0	2010
Bulgaria	100	100	100	0	2012	Slovenia	100	100	100	0	2011
Hungary	100	100	100	0	2011	Spain	100	100	100	0	2011
Austria	100	100	100	0	2011	Sweden	100	100	100	0	2011
Belarus	100	100	100	0	2012	Switzerland	100	100	100	0	2011
Belgium	100	100	100	0	2010	United Kingdom	100	100	100	0	2010
Canada	100	100	100	0	2012	United States of America	100	100	100	0	2009

Civil registration has a very important gender component. When it comes birth registration, beyond the newborn, the main emphasis is on the identity of the mother and to lesser extent on the father. While both parents are expected to participate in the registration and provide their identity data, where this is not the case the main responsibility lies with the mother to complete the registration. This task can become even more burdensome in instances where a child is born in a rural remote area and outside of a health facility. This often means that, in the absence of adequate facilitation by the authorities, a mother needs to take care of a newborn and also travel distances to implement the required registration procedures.

Similar situations can arise in relation with other types of registration such as marriage registration. It is often the case in some community traditions that women getting married will relocate to live with their husband's family. While all civil registration documents required for marriage in the case of the groom are already available at his place of residence, this may not be the case for a bride, who may be required to travel distances to obtain the certificates from the place of her residence necessary to register the marriage.

Finally, in terms of gender, civil registration faces numerous challenges in reflecting developments in society. In many countries sex can be changed and a person born with one sex can change gender and sex over time. This also has significant consequences in terms of recording registration of birth of newborn children of couples where one or both parents has undergone a sex-change at some point in time.

3.3. THE INSTITUTIONAL ARRANGEMENT OF A CIVIL REGISTER

All OSCE participating States have legal provisions to ensure that vital events are registered. Legislation specifies the type of vital events that must be registered, the time requirements for registration, the designated person or office responsible for registration and the place where the registration is to be carried out. In order to implement all necessary safeguards and manage the information in the civil register, administrative arrangements are also made to ensure that registered events and personal data are retained and stored in a format that allows for information retrieval and further processing. The institutional arrangements for the civil register vary among participating States.

In the OSCE region, the civil register is typically assigned to a ministry. Having sovereign authority to decide on the matter and in the absence of agreed international standards that establish structures for civil registration, different states have taken different approaches in appointing the authority responsible for civil registration. These range from an agency within the Ministry of the Interior or Ministry of Justice, to a specialised agency established for this function, depending on the country.

Structurally, the civil registry can be categorized as a centralized organization with decentralized functions, since authority to carry out civil registration has been delegated to local registrars. The practice across the OSCE region differs but, in general, both the civil registration system and the direction, co-ordination and supervision of local authorities responsible for civil registration are entrusted to either the Ministry of the Interior or Ministry of Justice.

TABLE 3.1 AUTHORITIES RESPONSIBLE FOR CIVIL REGISTRATION IN OSCE PARTICIPATING STATES

Participating State	Civil registration authority	CR system established
Armenia	Civil Registry Office, Ministry of Justice	1920
Azerbaijan	Ministry of Justice	1920
Finland	Maistraatit Magistraterna – Local Registry Offices	1923
France	Public Service, Municipalities, Bureau de l'Etat-Civil	1792
Georgia	Public Service Development Agency, Ministry of Justice	1919
Kazakhstan	Civil Registration Office, Ministry of Justice	1991
Latvia	Civil Registration Department, Ministry of Justice	1918
Lithuania	Civil Registry Offices, Ministry of Justice	1992
Mongolia	General Authority for State Registration, Ministry of Justice	1918
Russian Federation	Offices of Vital Records and Civil Registry Offices, Ministry of Justice	1917
Spain	Ministry of Justice	1870
Tajikistan	Civil Registration Office, Ministry of Health and the State Committee for Statistics	1995
Ukraine	District-level Civil Registry Offices, Ministry of Justice	1784
Uzbekistan	Civil Registry Office, Ministry of Justice	1992
Albania	Vital Statistics Offices, Ministry of Interior, General Directorate of Civil Status (GDCS)	1930
Austria	Ministry of Interior	1868
Belarus	Ministry of Interior	1917
Belgium	Municipalities, Civil Registration Departments	1796
Czech Republic	Civil Registry, Ministry of Interior	1946
Denmark	Population Register, Tax Administration, Ministry of Economic Affairs and the Interior	1874
Estonia	Vital Statistics Office, Ministry of Interior	1918
Germany	Standesamt/Civil Registry Office, Municipality, Ministry of Interior	1876
Iceland	National Register of Persons (Þjóðskrá), Ministry of Interior	1953
Italy	Register of Births, Marriages and Deaths (Registro Communale dello Stato Civile), Ministry of Interior	1804
Luxembourg	Municipalities, Ministry of Interior	1796
Former Yugoslav Republic of Macedonia	Ministry of Internal Affairs	1946
Montenegro	Ministry of Internal Affairs	1878
Netherlands	Bevolkingsregister, Ministry of Interior	1811
Poland	Ministry of Interior	1808
Portugal	Civil Assistance Centre (Loja do Cidadão), Directorate-General of Registries and Notaries, Ministry of Interior	1911
Romania	Municipalities, Office of Vital Records	1864

TABLE 3.1 AUTHORITIES RESPONSIBLE FOR CIVIL REGISTRATION IN OSCE PARTICIPATING STATES (CONT.)

Participating State	Civil registration authority	CR system established
Slovakia	Civil Registry Office, Ministry of Interior	1730
Slovenia	Ministry of Interior	1812
Turkey	Department of Civil Registration and Citizenship, Ministry of Interior	1884
United Kingdom	General Register Office, Home Office	1837
Ireland	Civil Registration Service, Health Service Executive	1864
United States of America	Offices of Vital Statistics in State Departments of Health	1946
Bosnia and Herzegovina	Municipality	2002
Bulgaria	Municipality	2000
Canada	Canadian Federation. Civil registration the responsibility of each province. Provinces/Territories > Vital Statistics or Service BC Offices	1864
Croatia	Municipalities, State Administration Offices	1946
Greece	Local Town Hall	1856
Hungary	Kozigazagatas, Municipality Registry Office	1895
Kyrgyz Republic	State Registration Service	1993
Moldova	Ministry of Information Technology and Communication	1993
Norway	Tax Administration, responsible for the National Population Register (national identity numbers)	1876
Serbia	Municipalities, Ministry of Local Self-Governance	1895
Sweden	Swedish Department of Tax, Ministry of Finance	1860
Switzerland	Registry Office (communal/cantonal/federal)	1798
Turkmenistan	Civil Registration Offices (district level)	1992

However, there are exceptions. In Norway and Sweden, for example, civil registration is operated by the national tax authorities. In the United Kingdom, it is the responsibility of the General Register Office. In Ireland, civil registration is co-ordinated by the health authorities. Finally, in the Western Balkans, civil registration is supervised by the Ministry of Public Administration in Croatia and by the Ministry of Local and Self-Government in Serbia. In Bulgaria, the authority over civil registration is entrusted to the Ministry of Regional Development and Public Works.

In North America, civil registration in Canada is the responsibility of the Office of the Registrar General working under authority of respective provincial authorities. In the United States, this is the responsibility of the Vital Statistics Department operated by each state.

In OSCE participating States in Central and North-east Asia, civil registration is generally entrusted to the Ministry of Justice, with the exception of Kyrgyzstan, where civil registration is under the authority of the State Registration Service.

3.4. ADMINISTRATIVE ARRANGEMENTS FOR KEEPING AND RETAINING CIVIL REGISTRATION RECORDS

Legislation on civil registration generally requires that, as part of the registration of a vital life event, a registration act be completed and the information recorded in the civil register. For each type of vital life event, there can be a separate register that permanently stores information on registered events. In an event-based registration system in its pure form, each event that affects a person's civil status is recorded at the place where the event occurred. A person's birth is recorded at the place of birth; marriage is recorded at the place of marriage.

Traditionally, registers have been kept as books in which registered events are entered chronologically. For each type of vital event, a separate book is maintained. Prior to the digitization of the process, vital life events were recorded in a two-book system, with the obligation to send one of the books to the central register at the end of the calendar year. When this rule was not followed, the result was that the registration records remained in the local civil registration office, and individuals would have to go back to that office to obtain copies of their records. There are some OSCE participating States that still rely on such two-book registration systems, but these are increasingly being phased out as information technology is gradually introduced.

At present, civil registration records in most OSCE participating States have been converted to an electronic format, and entering registration records into an electronic database is sufficient in many states, and no legal requirement exists with regard to keeping paper-based archives, not even for backup purposes.

Table 3.2 provides an overview of the extent to which civil registration data has been transferred into an electronic format based on responses received from the questionnaires. The table also points to some degree of overlap, as some states responded positively both in terms of having their civil registration data digitized or partially digitized.

TABLE 3.2 LEVEL OF DIGITIZATION OF CIVIL REGISTRATION RECORDS

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Is the archive related to the civil status registration digitized?	YES	12	29	**13**	**45%**
	NO	12	29	**6**	**21%**
	Partially	12	29	**11**	**38%**

The digitization of civil registers has led to a revolution in terms of processing civil registration data. Building on the established administrative and procedural frameworks for civil registration, states have also taken different approaches in terms of how civil registration information is organized in digital databases, including the determination of access rights to that information.

3.4.1. Local databases operating as part of a single network

In some states, registration services are digitized only at the level of local registries. This means that registration records are kept electronically as an electronic database. The structure of the electronic database often mirrors the structure of records from paper-based registration books. This also means that for each type of vital life event registration book, there is a corresponding electronic book constituting a component of a single database.

As a next step in the digitization process, in some states these local databases have been or are in the process of being upgraded to become part of a single network that enables information to be stored in other databases, as well as the sharing of data in line with the relevant national framework for data and privacy protection.

This level of digitization makes it possible to query certain registration information across a wide range of local databases to verify the existence of civil registration records, whether of births, marriages or deaths. However, this approach provides limited possibilities for conducting nationwide queries and checks against multiple entries.

This approach is characteristic of OSCE participating States with large populations and complex internal administration. Any further integration of networked local databases at the national level is often the subject of a political decision that reflects not only the interests of civil registration but also the relationships between different administrative levels within the state.

So far, the experience of states that have decided to interconnect their local civil registration databases shows that this is a lengthy process that has not yet been fully completed. The strategies of these states show, however, that ensuring the interconnectedness of all local databases through a single network platform remains their ultimate goal.

France – Electronic Data Exchange of Civil Status Data (COMEDEC)

In France, local civil registration databases are gradually being linked to a dedicated network for data exchange called COMEDEC (Electronic Data Exchange of Civil Status Data), which is implemented jointly by the National Agency for Secure Documents and the Ministry of Justice.

The system enables the electronic exchange of civil status data between the recipients of civil status data (passport issuing authorities and notaries) and the local civil registration authorities. Implementation of the COMEDEC network began in June 2012 with the connection of the first 16 pilot municipalities. The widespread deployment of the network started on 1 January 2014, and by mid-2017 approximately 50 per cent of all local civil registration databases had become part of the network.

The Law on Modernization of Justice in the 21st Century, enacted on 18 November 2016, requires municipalities to connect their civil registration databases to the COMDEC network by no later than 1 November 2018.

United States of America – The National Association for Public Health Statistics and Information Systems (NAPHSIS) (https://www.naphsis.org/)

NAPHSIS is the national non-profit organization representing the state vital records and public health statistics offices in the United States. NAPHSIS and its members work with a variety of partners to improve the efficiency and security of vital records operations in every state, plus the District of Columbia, New York City, Puerto Rico, Guam, American Samoa, the U.S. Virgin Islands and the Northern Marianas Islands.

NAPHSIS has developed and operates electronic systems for vital records offices that:
- Allow for the secure exchange of vital records and information among jurisdictions;
- Provide data to agencies that use information from birth and death records; and
- Support electronic verification and/or certification of vital event records.

NAPHSIS operates several systems that enable electronic registration of vital life events and the sharing of this information among different jurisdictions within the United States. Some of these systems also allow for exchange of birth registration and death registration information with neighbouring states.

The EVVE system, owned and operated by NAPHSIS, allows immediate confirmation of the legitimacy of an American birth certificate presented by an applicant to a government office anywhere in the United States. Authorized EVVE users send an electronic query to any participating vital records jurisdiction to either verify the contents of a paper birth certificate or to request electronic certification instead of the paper birth certificate. An electronic response from the participating vital records jurisdiction either verifies or denies the match with the official records. The EVVE system will also flag responses in which the person matched is actually deceased, an important step that prevents fraud.

NAPHSIS also operates the State and Territorial Exchange of Vital Events (STEVE) system. Using STEVE, civil registration authority belonging to specific jurisdiction can:

- Send vital records that pertain to residents in other jurisdictions so the home state's reports include these important data; and
- Send death information to the jurisdiction of birth so that birth certificates can be flagged as "deceased", an important step in preventing fraud and identity theft.

3.4.2. Central civil registration database linked with local databases

Many OSCE participating States have taken a further step in the digitization of their civil registration systems by establishing a central database that mirrors all vital life events registered at the local level. The information is collected directly from local databases and represents the aggregated compilation of all records of vital life events from the local level. In situations where the Internet or independent national infrastructure is well developed, the information at the local level is entered via a computer terminal directly into the central database. Depending on the provisions in place, local registrars can access all information in the central register originally entered by their local office and in certain instances the registration records entered by other local offices.

With such a system in place, the central authority can employ a wide variety of tools that enable registration authorities to assess and monitor the integrity of the overall system. This

means, for instance, that the authorities can verify whether multiple entries have potentially been made and if an event (e.g., a birth or death) is registered more than once but linked to different identities. The system is also capable of allowing other authorities and individuals to access the database in a regulated environment to verify the registration of certain vital life events. In practice, this often means that a person does not need to contact the local authority where their vital life event is registered to obtain a registration certificate and that the information can be obtained *ex officio.*

In Armenia, Croatia, the former Yugoslav Republic of Macedonia and Serbia, among other countries, there is a separate, centralized and digitized civil register. This register may or may not be directly linked to databases operated by other national identity management actors, primarily civil identification authorities. In Croatia, the former Yugoslav Republic of Macedonia and Serbia, the civil registration database is linked with other identity management actors that, in a regulated environment, can view and verify specific information in the central civil register.

3.4.3. Population register

The rapid development of information technology has also resulted in significant investments in innovative solutions to information management for public administration purposes. In most OSCE participating States, investments have been made to create an IT-based platform for collecting, processing and retaining up-to-date personal information that can then be shared with certain public administration authorities that need personal data in order to function properly, e.g., election authorities need people's personal data in order to assign them to voter lists. The sharing of such data normally requires that there either be a legal basis that allows for access to personal data or that the person whose personal information is processed gives their consent to the processing of their personal data for a specific purpose. At a certain point, it became apparent that too many public administration stakeholders working with the population were maintaining their own databases of their clients/beneficiaries, and that the information across all of these databases was not necessarily up to date. To address this problem, a concept emerged that envisaged the creation of a single database that would aggregate all the relevant identity information of every resident, including their place of residence and a set of other attributed information as required. Implementation of this concept resulted in the implementation of a state-wide population register to which different authorities contribute the registration information that they are responsible for under the law.

The first true population registers were established in Scandinavian countries, which recognized the value of the information that they maintain for the reporting of vital life statistics and for the tax authorities. In fact, even today, the respective Ministries of Finance in both Norway and Sweden are in charge of maintaining the population register.

Under the traditional concept of a population register, local civil registration authorities have a permanent online link to the population register and transfer all recorded vital events directly into the central database, while authorities in charge of the registration of individuals' place of residence enter information on everyone's place of residence. Depending on the legal provisions in place, some other personal information may also be added in the register.

A population register is an individualized data system, i.e., a mechanism for continuous recording and/or co-ordinated linkage of selected information pertaining to each member of a country's resident population that makes it possible to provide up-to-date information about the

size and the characteristics of the population. Thus, it is the result of a continuous process in which notifications of certain events, recorded originally in different administrative systems, are automatically and instantly used to update the population register on an ongoing basis.

An important characteristic of population registers is that there is a corresponding personal record for every physical person to which all registration events are added, thus allowing access to up-to-date information on the civil status, identity and place of residence of any citizen. The system further allows access to historical data, making it possible to reconstruct historical changes to one's personal information. In some systems, where legislation provides for it, information may be linked between parents and children, thus making it possible to fully reconstruct an individual's family tree.

The introduction of a population register follows two important principles: **each person gets only one record, and personal information is registered once and then used for multiple purposes**.

The principle of one record per person suggests that the information is organized in such a way that every resident can have only one identity and therefore only one corresponding personal record in the system. Safeguarding this principle also means that the system is designed with a view to preventing the creation of multiple and/or fraudulent identities. Practical implementation of this approach does not mean that there is one record for each person in the database that is updated on an ongoing basis. More often, information is recorded based on registered events, but using their unique identifier, a person's record can be reconstructed at any given moment in time.

The principle of a single registration having multiple purposes promotes the idea of using the population register as a provider of up-to-date personal information about residents to other bodies in the public administration, thereby eliminating the need for operating separate sector-based databases, which, in turn, increases the overall cost-effectiveness of public administration. In countries where the population register is used to aggregate and keep residents' civil registration and other identity information up to date, the population register is recognized as the only legally valid source of personal identity information.

The population register also brings additional benefits for residents, who can obtain certificates for various types of identity information and vital life events at any local office in the country without the need to travel to the location where the event was originally registered.

Over time, many OSCE participating States ventured into the development of a unified state-wide system for aggregation of the processing of identity information and associated vital life events. While there is a variety of approaches to the implementation of these systems, they are all commonly referred to as a population register.

As per the questionnaires returned, the following OSCE participating States indicated that their civil register is an integral part of a central state-wide population register: Belgium, Bosnia and Herzegovina, Bulgaria, Estonia, Georgia, Kyrgyzstan, Latvia, Liechtenstein, Lithuania, Luxembourg, Montenegro, Netherlands, Poland, Slovenia and Sweden.

Broadly speaking, a population register consists of identity information introduced through the process of civil registration, including all corresponding vital life events. In addition, each person's registered permanent or temporary place of residence is included. The scope of any additional information to be included in such a register is determined by national legislation.

The term "population register" has gained wider use and it is often being used to also describe a system of interconnected or interoperable databases which keep personal identity or

identification data often maintained by single authority. For instance, in Albania, Belarus, Czech Republic, Georgia, Kyrgyzstan, Liechtenstein, Montenegro, Slovakia, Slovenia, Switzerland, and Turkey, civil registration and civil identification are both functions of the Ministry of Interior or a specialized agency. This means that apart from civil registration records, the system that stores personal information either also contains information on issued official identification documents or is linked with the databases of issued official documents. This means that personal records will also contain or have access to a biometric identifier that makes it possible to link specific identity data with a physical person. This also means that if a person has not obtained a national identity card, no information exists that could be used to link the natural person with a specific identity in the register.

In practice, every OSCE state that operates a form of population register also provides mandatory identity cards to all citizens. Therefore, adult residents will have their biometric information in the register linked with their personal record. In terms of biometric information, authorities keep an individual's most recent photograph, as well as previously collected photographs.

In terms of technical implementation, each participating State has taken a different approach. Systems often mimic the existing administrative division in terms of responsibility for registration of specific types of information. In many instances, a single ministry or agency is legally put in charge of operating the register. Other ministries and/or institutions tasked with the registration of specific types of personal information then provide information for the population register. This is done either by linking local offices directly with the population register or by maintaining sectoral databases which are then continuously synchronized with the population register.

The implementation of a unified system does not, however, require the existence of an umbrella register that aggregates the data from other sectoral registers. In some instances, the system is implemented as a network of interconnected sectoral databases where the personal identity information of each person can be linked using their unique personal identifier.

The establishment and running of a state-wide population register, whether a centralized database or network of sectoral databases, has been coupled with the development of robust legislation and administrative regulations on data protection and protection of privacy. Such legislation and independent monitoring require that each public administration actor responsible for registration and entering data in the system have access only to the types of data that it can process under the law. Other data in the system must remain inaccessible. Furthermore, systems are designed to keep a log each time personal information is accessed, including the purpose of this access, and to allow for an audit either by the owner of the personal data or by an authorized independent body.

3.5. UNIQUE IDENTIFICATION NUMBER

The centralization of data and the digitization of entire systems resulted in a transition from event-based data management to the aggregation of registered events as part of personal files. This means that various registered events involving the same person that were often scattered across different registration books at different locations had to be linked somehow, which was the reason for the creation of personal files. Although several types of identity data (e.g., first name, family name, mother's or father's name, date of birth) can be used to look up all registered events involving the same person for the purpose of linking data within large-scale databases, this approach is not practical. Furthermore, there is always a risk that some personal information may be mistyped during registration, making it impossible to look up other events

involving the same person. Finally, there is a probability that, in some cases, different people might have identical personal information, which could result in a mistaken match.

To ensure unique and unambiguous searches for a specific identity, a unique identification number is assigned to each identity in the system, reinforcing the principle of one record per person. Based on the questionnaires returned, the following OSCE participating States reported issuing unique identification numbers: Albania, Andorra, Armenia, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Estonia, former Yugoslav Republic of Macedonia, Georgia, Hungary, Ireland, Italy, Kazakhstan, Kyrgyzstan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Norway, Poland, Portugal, Serbia, Slovakia, Slovenia, Spain, Sweden, Turkey and Ukraine.[3]

In all of these states, a unique identifier is issued by civil registration authorities immediately after, or in parallel with, birth registration. Following the registration of a birth, any subsequent request to update personal information or register a vital life event requires not only that identity information be presented but also that the individual's unique identifier be presented. The number follows the person from birth until death and enables an additional level of verification with every subsequent update in the civil register asking questions about previous registrations.

Unique identifiers are generally designed as a logical construct built around specific personal information (e.g., date of birth) and internally designed codes for certain types of identity data and a control number.

TABLE 3.3 UTILIZATION OF UNIQUE IDENTIFICATION NUMBER

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Is there a unique identifier or personal identification number (PIN) assigned to each person?	YES	1	40	**34**	**85%**
	NO	1	40	**6**	**15%**

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
If YES, the PIN is defined as:	Random number	7	34	**7**	**21%**
	Logical construct	7	34	**28**	**82%**

3 There are other OSCE participating States that use unique information numbers, such as: Azerbaijan, the Czech Republic, Denmark, Finland and Romania. Information on these states is not included in the statistical analysis as they did not submit completed questionnaires.

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
At what point of time is the identifier assigned to an individual?	At birth (entered in the civil register)	5	36	**31**	**86%**
	Upon first issuance of an identity/travel document	5	36	**7**	**19%**

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Is the same unique identifier used by other government services for keeping personal information in their databases?	YES	3	38	**29**	**76%**
	NO	3	38	**10**	**26%**

The introduction of a personal identifier makes it possible to search for every identity recorded in a database without any possibility of ambiguity and, to a certain extent, prevents the creation of multiple or fraudulent identities. By assigning an identifier at birth, no other new identifier can be subsequently added. The system also ensures that a unique identifier can be issued only at birth or following the successful completion of naturalization in the case of foreign-born citizens.

Responses from the participating States reveal that logical construct has generally been the preferred choice for unique identification numbers. There are historical reasons for such decisions. Unique identification numbers designed as a logical construct facilitate assigning, issuing and management of unique identification numbers. As the use of unique identification numbers has become standard practice in many states, concerns have been raised that identifiers designed as logical constructs can in fact reveal sensitive personal information and therefore could be seen contradicting trends to strengthen privacy and personal data protection policies. Furthermore, concerns have also been raised that persons familiar with the personal information of another individual can use that information to reconstruct part of the unique identification number which coupled with use of certain software and use of “brute force” hacking can lead to reconstruction of the full unique identification number. Therefore, the use of random numbers introduced in some countries has been proven to provide a greater level of protection against gaining unauthorised access through reconstruction of unique identification numbers, and at the same time avoiding the disclosure of personal information.

3.6. CROSS-BORDER ASPECTS OF CIVIL REGISTRATION

In many situations involving the verification of civil status, information can be verified through direct access to the relevant records in the civil register database. When it comes to verification of information stored in a database abroad, however, direct access is unavailable, as the information is under the authority of another state.

For foreign-born individuals in the process of registering vital life events that could affect their identity information (e.g., marriage or name change), in addition to presenting identification documents (a travel document or residence permit), civil registration certificates might need to be presented as well.

Civil status documents are not produced in the same way in all states, and unlike travel documents, there are no international standards that specify the layout of certificates or their security features. Furthermore, there can be legal incompatibility regarding the same type of civil status among different countries (e.g., a person in a same-sex marriage registered in one country might not be recognized as married in another country).

In Europe, for instance, this situation can affect an extremely high number of people. According to Eurostat and as presented in the Table 3.5, a relatively significant proportion of the population of EU and EEA member states were born outside of their state of current residence.[4] In situations such as entering into marriage, presenting proof of marriage, requesting permanent residence for a child born abroad, for this category of the population the authorities generally request certificates issued by the authorities of their country of origin. While most of their identity information is likely to remain consistent, challenges can arise related to the legalization of original documents, translation and transliteration and diacritical marks.

4 Eurostat, Foreign born population by country of birth, 2015, <http://ec.europa.eu/eurostat/statistics-explained/images/e/ee/Foreign-born_population_by_country_of_birth%2C_1_January_2015_%28%C2%B9%29_YB16.png>.

TABLE 3.4 PROPORTION OF FOREIGN-BORN PERSONS IN THE TOTAL POPULATION OF THE EU AND EEA MEMBER STATES (IN THOUSANDS)

	Total		Born in another EU Member State		Born in a non-member country	
	(thousands)	(% of the population)	(thousands)	(% of the population)	(thousands)	(% of the population)
Belgium	180.9	16.1	854.2	7.6	954.8	8.5
Bulgaria	123.8	1.7	43.9	0.6	79.9	1.1
Czech Republic	416.5	4.0	163.5	1.6	253.0	2.4
Denmark	595.9	10.5	202.8	3.6	393.0	6.9
Germany	10 220.4	12.6	4 010.4	4.9	6 210.1	7.6
Estonia	192.9	14.7	13.3	1.0	179.6	13.7
Ireland	749.9	16.2	445.4	9.6	304.5	6.6
Greece	1 242.9	11.4	345.7	3.2	897.3	8.3
Spain	5 891.2	12.7	1 981.2	4.3	3 910.0	8.4
France	7 908.7	11.9	2 184.6	3.3	5 724.0	8.6
Croatia	561.1	13.3	70.5	1.7	490.6	11.6
Italy	5 805.3	9.5	1 815.5	3.0	3 989.8	6.6
Cyprus	176.7	20.9	107.4	12.7	69.3	8.2
Latvia	265.4	13.4	28.3	1.4	237.1	11.9
Lithuania	136.0	4.7	19.2	0.7	116.8	4.0
Luxembourg	248.9	44.2	186.0	33.0	62.9	11.2
Hungary	475.5	4.8	309.6	3.1	165.9	1.7
Malta	42.4	9.9	20.1	4.7	22.4	5.2
Netherlands	1 996.3	11.8	532.3	3.1	1 464.0	8.7
Austria	1 474.6	17.2	677.3	7.9	797.3	9.3
Poland	611.9	1.6	249.0	0.6	392.9	1.0
Portugal	864.8	8.3	227.7	2.2	637.1	6.1
Romania	281.0	1.4	112.4	0.6	168.7	0.8
Slovenia	237.6	11.5	68.1	3.3	169.5	8.2
Slovakia	177.6	3.3	147.9	2.7	29.7	0.5
Finland	314.9	5.8	114.8	2.1	200.0	3.7
Sweden	1 602.5	16.4	519.2	5.3	1 083.3	11.1
United Kingdom	8 411.0	13.0	3 090.7	4.8	5 320.4	8.2
Iceland	39.1	11.9	26.0	7.9	13.1	4.0
Liechtenstein	23.8	63.7	8.1	21.7	15.7	42.0
Norway	746.4	14.4	339.1	6.6	407.2	7.9
Switzerland	2 258.2	27.4	1 364.3	16.6	893.9	10.9

3.6.1. Legalization of civil status documents

In general, civil status registry offices in Europe do not accept documents that are not duly and correctly legalized or notarized. In principle, documents coming from foreign countries intended for use in another country must be legalized (authenticated) and/or notarized by the respective foreign country. Authentication in this context is a governmental act by which a designated public official certifies the veracity of the signature and/or seal and the position of the official who executed, issued or certified (a copy of) a particular document.

Normally, there are two options to get documents authenticated. The first option involves authentication by the Ministry of Foreign Affairs of the state in which the document was issued and subsequent authentication by the consular authorities (embassy or consulate) of the receiving state. The person appointed at the Ministry of Foreign Affairs and their signature must be known to the consulate in that country so that authenticity can be confirmed. The official at the Ministry of Foreign Affairs may not know in person, or have on file, the names and signatures of every registrar in their country and may not be able to certify authenticity directly. For this reason, in many cases, internal procedures require a chain of additional seals and signatures before a document even reaches an official at the Ministry of Foreign Affairs.

The second option is slightly different: after authentication by the Ministry of Foreign Affairs of the country in which the document was issued, it is then sent to the embassy of the issuing country, and from there to the Ministry of Foreign Affairs of the receiving country. To shorten this procedure, all EU member states, as well as many other states, are party to the 1961 Hague Convention Abolishing the Requirement of Legalization for Foreign Public Documents. The convention stipulates that signatory countries agreed to mutually recognize each other's public documents if they have a special seal and stamp on it, a so-called "apostille". An apostille (French for "certification") is therefore a form of internationally recognized notarization and ensures that public documents issued in one signatory country will be recognized as valid in another signatory country. The sole function of the apostille is to certify the authenticity of the signature on the document in question, the capacity in which the person signing the document acted and the identity of any stamp or seal affixed to the document. The apostille must either be attached as an annex to the official document (an "allonge") or placed on the document itself by means of a stamp. An apostille is issued solely upon request.

An apostille is issued by a designated authority in the issuing state that is on file at The Hague. This may or may not be the Ministry of Foreign Affairs. In many countries, there are several authorities designated and formally authorized to issue an apostille. Once an apostille is attached, these documents need no prior legalization by an embassy or consulate to be sent through the consular system; they can be used directly.

The International Commission on Civil Status (ICCS)
http://www.ciec1.org

The International Commission on Civil Status (ICCS) is an international intergovernmental organization that was founded in September 1948 and has its seat in Strasbourg, France. The ICCS currently has 16 member states: Austria, Belgium, Croatia, France, Germany, Greece, Hungary, Italy, Luxembourg, the Netherlands, Poland, Portugal, Spain, Switzerland, Turkey and the United Kingdom. Cyprus, Lithuania, Slovenia and Sweden have observer status. The ICCS's aim is to facilitate international co-operation in civil-status matters and to improve the operation of national civil-status departments. To this end, it keeps documentation on legislation and case law setting out the law of its member states, provides those states with information and expertise, carries out legal and technical studies, prepares publications and drafts conventions and recommendations. Since 1948, the ICCS has adopted 32 multilateral conventions, which are legally binding instruments, and made nine recommendations.

The obligation of registration officials to provide notice of certain events, namely marriage or death, directly to the registration officials in the place of birth within eight days is the subject of ICCS Convention No. 3 on the international exchange of information relating to civil status, signed in Istanbul on 4 September 1958, to which Austria, Belgium, France, Germany, Italy, Luxembourg, the Netherlands, Poland, Portugal, Spain and Turkey are parties.

Document Information System Civil Status (DISCS)

DISCS was founded in 1999 and is a web-based reference system developed by the authorities of Australia, Canada, the Netherlands, Norway (Norwegian ID Centre) and the United Arab Emirates. The aim of DISCS is to aid in the verification of foreign and national documents that contain information about marital status, identity, citizenship and other information on the holder's identity. DISCS contains information about genuine and false breeder documents, among other things.

European Association of Civil Registrars (EVS)
http://evs-eu.org/

EVS was founded in 2000 and is a network organization that focuses exclusively on the exchange of information and best practices related to the fields of civil registration, family law, identity management and civil justice between legal, judicial and administrative authorities.

Current members include the associations of civil registrars from Belgium, Germany, Italy, the Netherlands, Poland, Romania, Scotland, Slovakia and Slovenia.

EVS plays a key role in informing and advising policymakers at both the European and national level to encourage further European integration and improve administrative life for European citizens.

The EVS has made several declarations and policy proposals:
- marriage law (Declaration of Graz);
- exchange of civil status records (Declaration of Noordwijkerhout);
- name law (Declaration of Engelberg); and
- parental law (Declaration of Ghent).

Legalization is where the state that produced a document verifies that the signature of the civil registrar who issued the document or extract is authentic. This verification is mostly carried out by the consular or diplomatic authorities of the state where the document must be provided, but sometimes that state will be satisfied with legalization by the authorities of the state of origin of the document.

Numerous bilateral or multilateral conventions have made legalization obsolete. However, only the Hague Convention of 5 October 1961 is universally recognized and ratified by all the EU member states, replacing legalization with an apostille issued by the competent authority of the state of origin of the document. Several ICCS conventions dispense with the legalization of those civil status documents between states, but they have been ratified by a limited number of countries.

3.6.2. Translation of official records

Translation problems are a significant issue given the diversity of languages in use across the OSCE region. As a general rule, in order to be used, civil status documents issued by a foreign authority must be accompanied by a translation, at least where the civil registrar does not understand the language used. Translations must, in most cases, be done by a translator approved and authorized by the local authorities, by consuls of the state of stay in the state of origin of the document or by consuls of the state of origin in the state of stay. This has long been a concern of the ICCS, which has produced a series of conventions on the issue of extracts from civil status records for use abroad.

3.6.3. Transliteration and diacritical marks

A problem associated with translation is the transliteration of names from one alphabet to another. This problem occurs every day with the various marks that exist in an alphabet, e.g., the Spanish tilde, the Polish ł, the French circumflex, etc. The ICCS adopted conventions that regulate this matter in the ICCS member states but it would appear that regulations are not equally applied in all member states. In other OSCE participating States this matter remains strictly regulated by national regulations based on the principles and rules designed by national experts.

Rules for transliteration of names for the production of travel documents and which are recommended by ICAO could be a solution in such circumstances. Civil registration authorities handling foreign issued civil registration certificates may benefit from the name transliteration introduced on the travel document as such transliteration is likely to follow recommendations set forth by the ICAO.

4. CIVIL IDENTIFICATION

The issuance of national identification documents, such as identification cards, passports and other travel documents, is an important responsibility of governments. It is also an integral part of the national infrastructure for identity management. Based on these documents, other government authorities and private entities, both national and international, make crucial decisions. While the civil registration framework provides for legal registration and certification of identity information, including certification of vital life events, the civil registration system cannot be used to securely link the identity information in the register with a specific person. Some form of biometric information such as a facial image, fingerprints or other information unique to the identity holder also needs to be recorded and linked with the identity information. That identity information, in conjunction with information on the individual's physical appearance, can be recorded on a secure medium that can then be used for identification purposes, that is to say, to verify that the person claiming a certain identity is indeed that person.

To facilitate identification in interaction between citizens and the authorities, as well as in private transactions, every state also operates a legal and administrative framework for civil identification. The product of the civil identification framework is generally an official identification document that can be used for secure identification both in an individual's home country (national identity card) and abroad (passport).

All OSCE participating States operate civil identification systems that issue travel documents (passports). At the same time, the majority of OSCE participating States also issue mandatory or optional national identity cards, with notable exceptions in the cases of Andorra, Canada, Denmark, the Holy See, Ireland, Turkmenistan, the United Kingdom and the United States, which do not issue national identity cards.

In the OSCE region, there are three distinct approaches to identification management that differ based on whether official national identity cards are issued or not:

- **Eight participating States do not issue national identity cards.** Other forms of identification are issued for sectoral purposes and in combination with other documents can be used as proof of identity (Andorra, Canada, Denmark, Holy See, Ireland, Turkmenistan, United Kingdom and United States of America).

- **Nine participating States issue national identity cards only upon request.** Highly secure national identity cards and travel documents are issued only upon a satisfactory in-depth verification of the applicant's identity (Austria, Finland, France, Italy, Lithuania, Monaco, Norway, Sweden and Switzerland).

- **Forty participating States issue mandatory national identity cards.** The identity of all adult resident citizens is established through detailed adjudication of official proof of identity (Albania, Armenia, Austria, Azerbaijan, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Italy, Kazakhstan, Kyrgyzstan, Latvia, Liechtenstein, Lithuania, Luxembourg, the former Yugoslav Republic of Macedonia, Malta, Moldova, Monaco, Mongolia, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Russian Federation, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Tajikistan, Turkey, Ukraine and Uzbekistan).

Considering that identification documents include important identity information duly registered following legal civil registration procedures, as well as information that links an identity with a person, these documents need to be secure and issued in a secure and accountable environment. Only identification documents issued through a procedure that demands trust and integrity can be accepted as genuine proof of identity.

The credibility of national civil identification systems relies partly on the authority that issues the documents, how they are organized, which infrastructure is in place and how the application and issuance processes are designed. Depending on the country and its administrative tradition, different authorities can be responsible for the issuance of documents. This could be the police, an immigration service, a civil organization based in a municipality, a passport office or a ministry. In a number of countries, there is also a clear distinction between the decision- and policy-making authorities and the operational part of the issuing process. The decision- and policy-making entity is usually a ministry, while the operational part of the issuing process is performed by civil servants in municipal or regional offices. In some countries, both qualifications are performed within the same office.

Unlike civil registration, where the issuance and design of civil registration certificates are matters of national regulation, the design of identification documents is regulated in great detail by relevant international standards. This is specifically the case with the design of travel documents, and it extends to national identity cards if they can also be used as a travel document based on bilateral or multilateral agreements. Most of the standards and recommended practices in this area have been adopted by the International Civil Aviation Organization (ICAO).

Most OSCE participating States issue far more national identity cards than travel documents. Where the use of national identity cards is mandatory (which is the case in 40 OSCE participating States), national identity cards are generally issued to nearly every citizen of the country, while only a certain percentage of the population needs a passport or travel document.

Research shows that 48 of the OSCE's 57 participating States issue identity cards, while nine states do not. In 40 states, identity cards are designed according to ICAO specifications, which means that they contain a machine-readable zone on the card. Among those 40 states, there are already 20 that have added a contact chip on their identity cards to facilitate other in-country processes. The content of the contact chip is mainly used in the issuing country for identity verification and e-services. To support facilitated cross-border travel, 13 states also have a contactless chip that is designed according to ICAO specifications and contains the same information as is stored in an e-passport.

The issuance of an identification document is only the end product of a larger process designed to ensure that cards are issued only to people who are entitled to one, with identity information that belongs to them.

The issuing process consists of three main parts:

- The application and verification process;
- The document personalization process; and
- Document delivery.

While all three components are critical for the operation of a civil identification system, from the point of view of identity management, how the application and verification processes are implemented is the most relevant aspect. The two other components are important from the point view of fraud prevention.

In terms of application and verification processes, there can be many different approaches depending on the legal framework for civil registration, the historical division of responsibilities among public administration actors, the size of the country, the information technology infrastructure, the level of adaptation to new technologies and a user-friendly application process for citizens.

Identification documents are generally valid only for a specific period of time. This means that a person will likely apply many times to obtain a new document after their previous one expires. The procedures for first applicants and returning applicants usually differ, especially in the range of verifications of their identity that need to be performed.

4.1. CIVIL IDENTIFICATION COVERAGE IN THE OSCE REGION

Unlike civil registration, where the registration coverage across the OSCE region is almost universal, the proportion of the population covered by civil identification varies from state to state. Tables 4.1 and 4.2 are compiled on the basis of information collected by the World Bank and show that a percentage of the population above the age when they become eligible for receiving an identification document (IDA) never obtain such a document. This also includes states where obtaining a national identity card is mandatory under the law.

TABLE 4.1 CIVIL IDENTIFICATION COVERAGE OF POPULATION ABOVE THE IDENTIFICATION ELIGIBILITY AGE IN OSCE PARTICIPATING STATES (INCLUDING DATA FOR MEN AND WOMEN)

Country	Registered Population above IDA	% of Population above IDA that is Registered	Registered Male	Registered Female	Country	Registered Population above IDA	% of Population above IDA that is Registered	Registered Male	Registered Female
Albania	2 248	77.2	n/a	n/a	**Lithuania**	2 327	82.2	n/a	n/a
Armenia	2 370	78.2	n/a	n/a	**Luxembourg**	576	98.6	289	287
Austria	8 630	97.9	4 229	4 400	**former Yugoslav Republic of Macedonia**	1 658	79.6	n/a	n/a
Azerbaijan	5 127	51.4	2 479	2 648	**Moldova**	3 964	97.8	1 895	2 043
Belarus	6 978	73.8	n/a	n/a	**Mongolia**	1 911	62.6	n/a	n/a
Belgium	11 268	98.5	5 538	5 730	**Montenegro**	487	77.8	n/a	n/a
Bosnia and Herzegovina	3 176	83.7	n/a	n/a	**Netherlands**	16 979	99.7	8 417	8 562
Bulgaria	5 849	83.0	n/a	n/a	**Norway**	5 258	98.6	2 649	2 609
Canada	25 940	70.8	12 870	13 070	**Poland**	30 709	79.6	n/a	n/a
Croatia	3 457	82.1	n/a	n/a	**Portugal**	8 546	83.3	n/a	n/a
Czech Republic	8 395	79.5	n/a	n/a	**Romania**	15 676	81.5	n/a	n/a
Denmark	5 749	100.0	2 860	2 889	**Russian Federation**	110 061	76.8	n/a	n/a
Estonia	900	68.9	n/a	n/a	**Serbia**	6 739	76.8	n/a	n/a
Finland	5 503	99.3	2 712	2 791	**Slovakia**	4 427	81.5	n/a	n/a
France	44 587	68.7	n/a	n/a	**Slovenia**	2 066	99.7	1 025	1 041
Georgia	3 140	79.1	n/a	n/a	**Spain**	34 634	75.2	16 766	17 869
Germany	81 752	100.0	40 247	41 505	**Sweden**	9 995	100.0	5 013	4 982
Greece	9 005	82.7	n/a	n/a	**Switzerland**	8 237	97.4	4 077	4 160
Hungary	8 075	82.5	n/a	n/a	**Tajikistan**	4 402	49.7	n/a	n/a
Iceland	247	73.7	123	124	**Turkey**	54 050	67.2	n/a	n/a
Ireland	4 758	99.9	2 352	2 406	**Turkmenistan**	3 252	59.1	n/a	n/a
Italy	46 715	78.1	22 465	24 250	**Ukraine**	34 671	78.1	n/a	n/a
Kazakhstan	9 819	54.4	n/a	n/a	**United Kingdom**	46 500	71.0	n/a	n/a
Kyrgyz Republic	2 852	46.6	1 340	1 512	**United States of America**	157 596	48.3	73 761	83 835
Latvia	1 554	79.9	n/a	n/a	**Uzbekistan**	20 435	66.6	n/a	n/a

Using the data published by the World Bank, Table 4.2 provides an overview of the size of population that has not been issued a national identity card or other forms of identification in cases where a national identity card is not mandatory. The table provides gender-disaggregated data, highlighting the proportion of women in the overall population without identification.

TABLE 4.2 THE PERCENTAGE OF THE POPULATION OF OSCE PARTICIPATING STATES WHICH DID NOT RECEIVE AN OFFICIALLY-ISSUED FORM OF IDENTIFICATION (INCLUDING PERCENTAGES FOR WOMEN)

Country	Unreg. Population (k)	% of Country Population Unreg.	% Unreg. Population that is Female	Unreg Females as % of Total Pop	Country	Unreg. Population (k)	% of Country Population Unreg.	% Unreg. Population that is Female	Unreg. Females as % of Total Pop
Albania	9	0.30	n/a	n/a	Lithuania	-	0.00	n/a	n/a
Armenia	3	0.10	n/a	n/a	Luxembourg	8	1.35	43.69	0.59
Austria	184	2.09	43.53	0.91	Former Yugoslav Republic of Macedonia	1	0.05	n/a	n/a
Azerbaijan	2.370	23.76	50.83	12.08	Moldova	91	2.23	71.55	1.60
Belarus	640	6.76	n/a	n/a	Mongolia	142	4.64	n/a	n/a
Belgium	176	1.54	36.42	0.56	Montenegro	1	0.14	n/a	n/a
Bosnia and Herzegovina	3	0.07	n/a	n/a	Netherlands	54	0.32	18.13	0.06
Bulgaria	0	0.00	n/a	n/a	Norway	72	1.36	46.57	0.63
Canada	3.628	9.91	53.60	5.31	Poland	990	2.57	n/a	n/a
Croatia	75	1.79	n/a	n/a	Portugal	-	0.00	n/a	n/a
Czech Republic	279	2.64	n/a	n/a	Romania	356	1.85	n/a	n/a
Estonia	158	12.07	n/a	n/a	Russian Federation	4.310	3.01	n/a	n/a
Finland	38	0.69	51.57	0.35	Serbia	320	3.65	n/a	n/a
France	6.084	9.37	n/a	n/a	Slovakia	20	0.37	n/a	n/a
Georgia	3	0.08	n/a	n/a	Slovenia	5	0.26	56.88	0.15
Germany	-	0.00	0.00	0.00	Spain	11.436	24.82	49.10	12.19
Greece	-	0.00	n/a	n/a	Sweden	-	0.00	0.00	0.00
Hungary	0	0.00	n/a	n/a	Switzerland	217	2.57	47.44	1.22
Iceland	8	2.36	49.05	1.16	Tajikistan	1.265	14.29	n/a	n/a
Italy	3.312	5.54	51.64	2.86	Turkey	2.540	3.16	n/a	n/a
Kazakhstan	2.599	14.39	n/a	n/a	Ukraine	1.772	3.99	n/a	n/a
Kyrgyz Republic	1.067	17.42	47.01	8.19	Uzbekistan	5	0.02	n/a	n/a
Latvia	46	2.34	n/a	n/a					

4.2. AUTHORITY IN CHARGE OF ISSUING IDENTIFICATION DOCUMENTS

OSCE participating States, starting with their administrative decisions, take different approaches in terms of the authorities designated for the issuance of identification documents. Based on the information obtained via questionnaires, in most participating States, the Ministry of Interior is responsible for handling the issuance of identification documents. It is also true that it is not always the same authority that is in charge of issuing all official identification documents (national identity cards and passports) and that these responsibilities might be shared among several different government authorities. Information presented in Table 4.3 shows

that in most OSCE participating States it is the Ministry of Interior that is responsible for civil identification. Some participating States appointed the Ministry of Justice as the responsible authority or decided to establish an altogether separate agency tasked with civil registration and identification issues.

TABLE 4.3 AUTHORITIES IN CHARGE OF ISSUANCE OF NATIONAL IDENTITY CARDS

Country	National Identity Card (NIC) Issuing Authority	NIC system established YYYY	NIC card name	NIC eligibility age
Albania	General Directorate of Civil Status, Ministry of Interior	2012	Letërnjoftimi/Albanian Identity Card	16
Armenia	Police Department, Ministry of Interior	1991	National Identity Card/National Passport	16
Austria	Ministry of Interior	2005	Identitätsausweis/Personalausweis (Austrian Citizen Card)	-
Azerbaijan	Ministry of Interior	1994	Azərbaycan Respublikası vətəndaşının şəxsiyyət vəsiqəsi (National Identity Card)	16
Belarus	Ministry of Interior	1923	National Passport	16
Belgium	National Register, Municipalities	2000	BelPIC/Identiteitskaart/Carte d'Identité /Personalausweis (Identity Card)	12
Bosnia and Herzegovina	Ministry of Internal Affairs	2001	Lična Karta (Identity Card)	16
Bulgaria	Ministry of Interior	1999	Лична карта (Identity Card)	14
Croatia	Police Department, Ministry of Interior	2003	Osobna Iskaznica (Identity Card)	16
Czech Republic	Ministry of Interior	1939	Občanský Průkaz (Identity Card)	15
Estonia	Police and Border Guard Board	1993	ID-kaart/National Identity Card	0
Finland	Police	2003	FINEID/Identification Card (Henkilökortti/Identitetskort)	-
France	Police (Paris)/Mayor's office in the town of residence (France, except Paris)	1980	French National Identity Card	16
Germany	Municipality, Ministry of the Interior	2010	Personalausweis (Identity Card)	16
Greece	Police Department, Ministry of Interior	2005	Αστυνομική Ταυτότητα/National Identity Card	12
Hungary	Office of Immigration and Nationality, Ministry of Interior	2001	Személyi Igazolvány/Identity Card	14
Iceland	National Register of Persons ("Þjóðskrá"), Ministry of Interior	1962	Nafnskírteini/National Identity Card	14
Italy	Ministry of Internal Affairs	2001	National Identity Card	15
Latvia	Office of Citizenship and Migration Affairs, Ministry of Interior	2006	Personas Apliecība (National Identity Card)	18
Lithuania	Ministry of Interior	2009	Asmens Tapatybės Kortelė (Identity Card)	16
Luxembourg	Municipalities, Ministry of Interior	2014	Carte de Identite (Identity Card)	15
Former Yugoslav Republic of Macedonia	Ministry of Interior	2008	Лична карта (National Identity Card)	18
Montenegro	Ministry of Internal Affairs	2008	Lična Karta (Identity Card)	16
Netherlands	Municipality (mainland)/Island administration (overseas territories)	1850	Identiteitskaart (Identity Card)	14

Country	National Identity Card (NIC) Issuing Authority	NIC system established YYYY	NIC card name	NIC eligibility age
Poland	Office of Civic Affairs, Ministry of Interior	2002	Dowód Osobisty (Identity Card)	18
Romania	Ministry of Administration and Interior	1949	Carte de Identitate (Identity Card)	14
Russian Federation	Federal Migration Service, Ministry of Interior	1992	Универсальная электронная карта (Universal Electronic Card)	16
Serbia	Ministry of Interior	2004	Lična Karta (Identity Card)	10
Slovakia	Police Department, Ministry of Interior	2008	Občiansky Preukaz (Identity Card)	15
Slovenia	Ministry of Interior	2008	Osebna Izkaznica (Identity Card)	18
Spain	National Police	2006	Documento nacional de identidad (National Identity Card)	14
Sweden	National Police	2005	Nationellt id-kort (National Identity Card)	-
Tajikistan	Ministry of Internal Affairs and Communications	2014	National Identity Card	16
Turkey	Department of Civil Registration and Citizenship, Ministry of Interior	1974	Nüfus Cüzdanı/National Identity Card	0
Ukraine	State Migration Service of Ukraine, Ministry of Interior	1994	Ukrainian National Passport	16
Georgia	Public Service Development Agency, Ministry of Justice	2011	National Identity Card	14
Kazakhstan	CON Registration Office, КЕАК	1997	Жеке куәлік (Identity Card)	16
Mongolia	General Authority for State Registration, Ministry of Justice	1999	National Identity Card	16
Kyrgyzstan	State Registration Service	2009	National Identity Card	16
Moldova	Ministry of Information Technology and Communication	1996	Buletin de identitate (Identity Card)	0
Norway	Norwegian Tax Administration	-	National Identity number	-
Portugal	Agência para a Modernização Administrativa, Council of Ministers	2008	Cartão de Cidadão (Citizen Card)	10
Switzerland	Canton/Municipality	1955	Identitätskarte (Identity Card)	-
Uzbekistan	Department of Visas and Registration, Ministry of Foreign Affairs	1995	National Passport	16

Across the OSCE region, it is not uncommon that more than one identity management function is the responsibility of a single authority. For instance, in many participating States the same authority (e.g., Ministry of Interior) is responsible for issuance of national identity cards and travel documents (e.g., Austria, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Finland, France, Greece, Latvia, Lithuania, Romania, Serbia, Spain, Sweden and Ukraine). Furthermore, in some participating States, the same authority (Ministry of Interior) is not only responsible for issuance of national identity cards and travel documents but also has responsibility for the conduct of civil registration (e.g. Albania, Belarus, the Czech Republic, Montenegro, Slovakia, Slovenia, Switzerland and Turkey).

4.3. APPLICATION AND VERIFICATION PROCESS

Regardless of the authority in charge of the issuance of either national identity cards or passports, whichever is issued first, all authorities generally follow a similar approach to the issuance of these documents, where the application and verification process is arguably the most important of the four components in the entire process.

The purpose of an identification system is to ensure that a link is created between a person and their identity information; that this identity information is already legally recognized during the registration procedure; that information on the person's physical attributes is collected, stored and retained in a database; and that a secure identification card is issued with that information. That identification card is subsequently used as legal proof of identity and as an instrument to determine that the holder of the document is in fact the owner of that identity.

The most critical part of this process is to ensure that the identity information provided during the application process is valid and that it belongs to the person who is claiming that identity. In order to ensure secure identification in the application process, the authorities develop processes through which they request and verify relevant evidence of identity in order to make sure that the identity exists, that it is the identity of a living person and that the identity is in wide use.

Obtaining appropriate evidence to determine the validity of an identity implies determining that the identity exists, that the identity is that of a living person, that the applicant is linked to the identity, that the applicant is the sole claimant of the identity, and that the identity is in use in the community.

In practice, obtaining evidence that an identity exists means that the identity is recognized and registered by the state, including by going as far as to the point of birth when a person's identify is recognized and registered for the first time. Other documents issued based on breeder documents (mainly birth certificates) may also prove that an identity exists.

A person may present proof of identity, and the verification may prove that the identity exists. However, that identity may belong to a person who is no longer alive and is being used to obtain identification documents under multiple identities. The death records in the civil register can be a reliable resource for verification, including in combination with testimony from witnesses. The issue may be more pertinent in instances where the authorities allow remote applications for the renewal of documents.

Finally, while it can be established that an identity exists and belongs to a living person, it is equally important to verify whether the identity is in wide use in society. This requirement is in recognition of the fact that the civil register of any state may contain information about the identities of individuals who are still living but who may have left the country or who have not requested official or other forms of identification documents for a long period of time. Such identities may also be used for the purpose of obtaining multiple identification documents using different identities.

In addition to proof of identity, authorities also require proof of citizenship, which is a determining factor in deciding if a person is entitled to a national identity card. Depending on citizenship legislation, it can be the case that a birth certificate alone is sufficient, while many states maintain a separate register of citizens for those who qualified for citizenship at birth,

which also contains additional information about individuals who became citizens through the naturalization process.

The practice of OSCE participating States suggests that different approaches are usually taken depending on whether the applicant is a first-time applicant or is applying to renew a document. The following principles are valid and need to be fulfilled regardless of whether an applicant is a first-time applicant or a returning applicant.

The first step is to check that the person claiming the identity is a citizen and qualifies for an identification document. Depending on the type of document issued, identification documents are used to verify if a person is a citizen or not and, in the case of non-citizens, their legal residence status in the state.

The second step in the process focuses on identity verification based on documentary evidence provided as part of the application. The types of documentary evidence required from the applicant vary among states and depend on the national identity management infrastructure.

The third step is to establish and verify the link between the physical person and the claimed identity by collecting and storing required biometric identifiers.

4.4. DOCUMENTARY EVIDENCE REQUIREMENTS

The practice of OSCE participating States indicates that all applicants must provide certain documentary evidence to obtain a national identity card or passport. The application information backed by documentary evidence is then examined to determine whether a person is entitled to an identification document. In this phase, officials from the issuing authority have to find evidence that the identity indeed exists and, secondly, that the identity belongs to the person who applied for the document.

A number of instruments of documentary evidence can be requested to help officials complete the identity verification process. The following represents an overview of some good practices from OSCE participating States in designing the application process, the documentary evidence required and the verification of the supplied identity information.

Belgium

- The person applying has to be present (except children younger than six years of age living abroad);
- Birth certificate as proof of official identity. For children born in Belgium, the parent(s) and the doctor, hospital or the midwife who assisted with the childbirth have to report the birth independently, which provides double verification;
- Interview on the basis of identity data regarding the person and their family; and
- Identification documents from another country if the person also has another citizenship.

Canada

- Original documentary evidence of citizenship (birth certificate or citizenship certificate) and at least one piece of federal or provincially issued supplementary identification;
- Security features verified on the original documentary evidence of citizenship;
- Documentary evidence of citizenship verified against citizenship database; and
- Documentary evidence of citizenship information compared with supplementary evidence of identity;
- Facial recognition software used to determine uniqueness of identity;
- Client photograph compared to identification, personal appearance (if applicable), also against database if applicable;
- Applicant information (surname and date of birth) run through database to determine uniqueness of identity;
- Trusted referees contacted if applicant meets certain risk-based criteria;
- Photographs verified by guarantor to ensure they represent a true likeness of the applicant; and
- Facial recognition queried one to many to ensure uniqueness of identity.

* Process applicable to people 16 years of age and above.

Croatia

The person must present proof of Croatian citizenship and a public document with a photograph or document issued by a state authority if the person has already been issued a public document. If the person has not been issued any public document, their identity must be confirmed by adults who they know and whose identity has been previously checked. If it is not possible to determine the identity of the person making the request for the identity card or passport in this way, their identity is determined by police officers through the procedure stipulated by a special regulation.

Estonia

First-time applicants have to apply in person. A legal representative must submit an application on behalf of a minor under the age of 15 or a person under guardianship.

The applicant's facial image is compared against existing images in the national registry of personal identity documents;

If a person has a personal identity number, personal data will be compared to the data in the population registry. If a person does not have a personal identity number, then residence information will be checked from the population registry;

In case of doubt, an officer can verify the authenticity of a foreign document for European Union citizens and non-European Union residents by using document scanners;

If the data in the population registry is different from on the application, an officer will identify the correct information and record it in the remarks field in the system; and

If a person is over 18 years of age and has no previous documents issued in any country, an identity establishing protocol is in place. Information (e.g., citizenship, nationality, native language, education, marital status, family members, relatives) will be collected for the individual's file by interviewing the person and making inquiries.

Supporting documentary evidence:
- If a child was born in a foreign country, then the child's birth certificate needs to be submitted;
- Documents confirming or proving the right to Estonian citizenship;
- If the name of the parent in the birth certificate and in the identity document of the parent are different (the name of the parent was changed in a foreign country, and the changed data has not been entered in the Estonian population register), a document proving the name change (e.g., marriage certificate) needs to be submitted; and

A document evidencing the applicant's state of health, certifying that the applicant is unable to visit a service bureau (e.g., a medical certificate).

Georgia

For the issuance of a national identity card or travel document for the first time, a person should apply to the public service hall at any territorial office of the issuing authority and/or a community centre and present an identity document (birth certificate, marriage certificate, other identity document issued by a foreign country, passport issued by former Soviet authorities if the document is to be issued for the first time, a document necessary for determination of citizenship and a photograph). An application is accepted through the agency's special software. The presented documents are initially considered and compared by the front office with the data in the agency's database. The front office also enters the data in accordance with the provided documents and information and registers the application. If no record is available of a previously issued photograph document, a person's photograph is verified by another adult.

Subsequent to registration, the application is forwarded to the back office for consideration. Identity documents submitted by a person are considered by the back office. Information specified in the presented documents is compared with the data in the agency's electronic database and material archives. Civil status records registered in the name of the person are retrieved, and if the person's civil status records are registered abroad, the applicant must provide an apostille or legalization for the documents evidencing the aforementioned information. The legitimacy and authenticity of the data is determined. The presented photograph is compared with other photographs in the agency's electronic database to ascertain whether a document has already been issued to the person. If necessary, the back office will collect additional documents from different public agencies and/or a foreign country.

To determine citizenship, information may be requested (as a certificate) from the relevant self-government agency in accordance with the place of residence of the person for the purpose of ascertaining the fact of their residence. Information about whether the person is wanted for committing a crime is checked against the database of the Ministry of Internal Affairs. For a travel document to be issued to the person, the person should be registered and/or hold an identity card/residence card. Subsequent to study and a comparison of the documents, the relevant decision is made. In case of a positive decision, the application is forwarded to the printing centre for personalization.

Hungary

Identity document requirements:
- Birth certificate, marriage certificate appropriate for determining the applicant's name;
- Immigrants, individuals recognized as refugees, foreign citizens with protected legal status and non-citizen permanent residents are required to present the following documents: immigration permit, documents certifying recognition of refugee and protected legal status, or a document certifying residence status for non-citizens and an official certificate of their personal identifier and address of domicile; and
- An identity card photograph for refugees and foreign citizens with protected legal status. On the back of the identity card photograph, the competent authority indicates the number of the document certifying recognition of the refugee and protected legal status and verifies the identity of the person applying with a signature and official seal.

Passport requirements:
Address card (official certificate of an individual's personal identifier and address of domicile) if the applicant has:
- a birth certificate or marriage certificate if they do not have any document for personal identification or if the information in the personal data and address register does not correspond with the information on the document or deed; and
- in the case of an applicant living abroad: a deed certifying Hungarian citizenship (endorsed naturalization document, citizenship certificate not more than three years from the date of issue) if they do not have any valid document appropriate for personal identification (e.g., national identity card, passport) or if the personal data and address register of citizens does not consider them to be a Hungarian citizen.

Hungarian citizenship may be attested by:
- a valid Hungarian identity card;
- a valid Hungarian passport;
- a valid citizenship certificate; and
- a certificate of naturalization – until proven otherwise.

If a Hungarian national cannot attest to their Hungarian citizenship by means of the above documents, Hungarian citizenship can also be attested by an expired Hungarian passport – until proven otherwise – for up to one year after its expiration. The register of personal data and addresses confirms the Hungarian citizenship of Hungarian citizens on file therein.

If the applicant falls within the scope of the personal data and address register, a travel document will be issued based on the particulars from the personal data and address register.

The Netherlands

- The applicant is asked to identify themselves based on an official identity document (e.g. driver's licence);
- If there is no identity document, a civil servant consults the applicant's personal data stored in the population register;
- The applicant has to answer identifying questions presented by a civil servant;
- If there is no doubt about the identity of the applicant, the application will be processed; or
- If there is doubt about the identity of the applicant, a second (back office) civil servant asks additional identifying questions.

Poland

Passport requirements:
- Application and collection in person (except children under five years of age);
- Identity verification on the basis of a previously issued national identity card;
- If a person does not have a national identity card, identity verification is carried out on the basis of different state registers and another document with a photograph; and
- If there is any doubt or inconsistency in the evidence presented above, the passport authority may require that an extract of a Polish birth record and confirmation of Polish citizenship be provided.

National identity card requirements:
- Application and collection of the document in person;
- Identity verification on the basis of a passport; and
- Identity verification on the basis of state registers.

If there is any doubt or inconsistency in state registers, the authority may require that an extract of a Polish birth record and confirmation of Polish citizenship be provided.

Serbia

A request for issuing an identity card, as well as for a passport, for a minor who does not have proof of identity must be submitted by one of the parents with written consent provided by the other parent, or other legal representative or guardian, which confirms the identity of the minor. In addition to the request, the following must be submitted: the identity card of the parent(s), legal representative or guardian. Data regarding the birth certificate and citizenship are obtained *ex officio* with the need for their consent.

When submitting a request for the issuance of an identity card for an adult who does not possess proof of identity, their identity can be established through statements by a person whose identity has been checked. In addition to the request, one must submit: a statement that their identity has been checked, and the identity card of a person whose identity has been checked. Data regarding the applicant's birth certificate and citizenship are obtained with their consent.

When submitting a request for the issuance of a passport for an adult who does not possess a previously issued identity card, their identity is checked using a document with a photograph that is issued by the competent state authority. This must be enclosed with the application.

4.5. GENERAL METHOD OF THE VERIFICATION PROCESS

Good practice from a number of OSCE participating States suggests that the documentary evidence issued by national authorities is generally additionally verified. There are two reasons for this. One is that, in general, civil registration certificates are not necessarily sufficiently secure documents and, second, that the shift towards the digitization and computerization of civil registration records has opened up the possibility for instant online verification of information in the civil registration records.

For a number of reasons, first-time applications are managed differently from document renewal applications. When an application is received for the first time, the issuing authorities, in many cases, do not have information on the identity of the person and must request legal proof of identity and verify, through due process, that the identity exists, is that of a living person and is in wide use. This process allows the authorities to enter in the database of issued identification cards identity information that is legally valid at the time of submission of the application.

The second critical aspect for first-time applicants is the lack of evidence that can be used to link an identity to the physical person claiming the identity. While for returning applicants, this information is already available in the relevant databases, for first-time applicants the link must be established through due process.

For returning applicants, the verification aspects of the application process are simplified, as the information verified during the first application already exists in the system and can be used as a point of reference for verification of the applicant's identity data, as well as of specific physical attributes such as face matching and or fingerprint matching.

Citizenship verification

The procedures for the issuance of identification and travel documents are designed largely to cater to the needs of citizens. Identity and travel documents are also issued to resident non-citizens, who may fall into different categories. However, different procedures apply in such cases and are elaborated in more detail in the section on identity management for resident non-citizens.

With differences in terms of an individual's eligibility for application for an identification document, proof of citizenship determines which type of identity or travel document an applicant is qualified to receive. For this purpose, documentary evidence presented as proof of citizenship varies across the OSCE region, but is provided in the form of a certificate with various security features.

4.6. IDENTITY VERIFICATION FOR FIRST-TIME APPLICANTS

The identity verification process is designed to detect any attempts at identity fraud that rely on possible gaps in the security of breeder documents. As part of this process, the authorities need to carefully trace all evidence of an applicant's identity to make sure that the identity exists as a legally recognized identity and that the identity is linked to the person applying for the identification document.

In general, participating States can face three distinct types of applications for identification documents, and a different set of processing rules apply for each type:

- First-time applications for national identity cards or travel documents for minors;
- First-time applications for national identity cards or travel documents by adult citizens; and
- Applications for renewal of national identity cards or travel documents.

Since most OSCE participating States issue national identity cards as a mandatory document or upon request, the first issuance of a travel document benefits from identity verification conducted during the issuance of a national identity card.

4.6.1. First-time application for national identity cards or travel documents for minors

In case of an application for a travel document for a minor or a first-time application for a national identity card by a minor eligible for a national identity card, whichever is first, authorities, as a general rule, require the presence of the applicant and the presence of at least one of the applicant's parents as shown in Table 4.4.

TABLE 4.4 REQUIRED PERSONS TO BE PRESENT FOR APPLICATIONS FOR MINORS

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
In the case of children, is the presence of the mother, father or both parents/legal guardians required?	YES	0	41	**39**	**95%**
	NO	0	41	**3**	**7%**

In countries that do not issue national identity cards, it can be very cost-ineffective to operate a large number of passport offices that are accessible to all applicants. This is particularly evident in a situation where the number of annual applications for travel documents is not very high. In such circumstances, the authorities allow remote applications for travel documents (including first-time applications) and apply a somewhat different approach to identity verification by conducting **social footprint checks**. This approach is widely used in the United States and the United Kingdom.

Information from birth records, whether presented as a birth certificate or by checking the database of birth records directly, is the most important evidence of identity. The practice in many OSCE participating States reveals that, in the majority of cases, the information provided via a birth certificate is also further verified directly in civil registration records.

If birth certificates are issued by foreign authorities, the expectation is that the certificate must be duly legalized in line with relevant procedures. Some of the good practices in this area are further elaborated in the section on civil registration.

The application for a national identity card or a passport is normally submitted by one of the minor applicant's parents or legal guardians. They either submit the child's photograph or bring the child in person to have their photograph taken. Verification as to whether the child is linked to the identity on the presented birth certificate is conducted by checking the identification documents (national identity card or travel documents) of the parents or legal guardian and making sure that the identity information matches the parental information printed on the birth certificate.

The identification document presented by the parents/legal guardians can additionally be verified by looking up their information in the source database of issued national identity cards/travel documents or by using different types of document scanners to look for the presence of distinct security features.

4.6.2. First-time application for national identity cards or travel documents for adults

In the case of first-time adult applicants, proof of identity comes in the form of certificates and documentary evidence submitted in line with the national requirements for the submission of supporting documents. The practice in many OSCE participating States demonstrates that these documents are not necessarily taken at face value. When compared with the investments and progress achieved with regard to the security of national identity cards and travel documents, the supporting documents required for application for an identification document do not meet the same security standards. As Table 4.5 shows, OSCE participating States increasingly rely on direct online verification of the data from documentary evidence in the source databases rather than investing in the security of the certificate documents.

TABLE 4.5 VERIFICATION OF INFORMATION SUBMITTED THROUGH DOCUMENTARY EVIDENCE

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Do you verify independently and ex-officio with the issuing authorities relevant information submitted as documentary evidence?	Verified only during first issuance	1	40	**3**	**8%**
	Verified during first and all subsequent issuances	1	40	**22**	**55%**
	Verified only in case of doubt about the legitimacy of submitted documents	1	40	**18**	**45%**

In practice, this means that the authorities carry out obligatory verification of identity data in civil registration databases, which helps to confirm without doubt that an identity exists by

looking at birth and marriage records and confirming that the identity is that of a living person by consulting records of deceased persons in the civil registration database. Table 4.6 suggests that there is a growing trend to develop direct online links between civil identification and civil registration databases to help with identity data verification. It further shows that the priority is given to enabling links to birth records and records of deceased persons.

TABLE 4.6 USE OF MANDATORY ONLINE VERIFICATION

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Automatic and mandatory online verification	Civil register (birth records)	0	41	**29**	**71%**
	Civil register (deceased persons)	0	41	**28**	**68%**
	Civil register (marriage records)	0	41	**20**	**49%**

As shown in Table 4.7, reliance on paper records is generally lower, which highlights a trend towards interconnecting various databases maintained by different authorities that process personal data.

TABLE 4.7 USE OF MANDATORY VERIFICATION IN PAPER RECORDS

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Mandatory verification in paper records	Civil register (birth records)	0	41	**8**	**20%**
	Civil register (deceased persons)	0	41	**4**	**10%**
	Civil register (marriage records)	0	41	**7**	**17%**

Establishing that the identity claimed by a person actually exists is generally coupled with verification that the identity belongs to a living person. Automatic verification, as Table 4.6 shows, is possible in cases where the existing infrastructure makes it possible to look up a specific identity in the records of deceased persons within the civil register electronic database.

The information presented in Table 4.8 further highlights the increasing trend towards the use of systematic online verification. As the table shows, less frequent verifications are carried out, usually only in cases where there is doubt about the validity of the supporting document submitted.

TABLE 4.8 USE OF VERIFICATION ONLY IN CASES WHERE DOUBTS HAVE BEEN RAISED

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Verification conducted only in cases of doubt	Civil register (birth records)	0	41	**8**	**20%**
	Civil register (deceased persons)	0	41	**9**	**22%**
	Civil register (marriage records)	0	41	**9**	**22%**

In countries where a unique numeric identifier is assigned at birth, this identifier makes it possible to look up and unambiguously confirm an applicant's identity using information about that identity stored in civil registration records. Where a unique identifier is not issued, looking up specific identities across different databases is more time-consuming.

If a person is applying for a travel document and has previously obtained an official national identity card, the presented national identity card can be verified by directly accessing the database of issued national identity cards and verifying the information at the source. If access is not possible, special scanners are normally used to verify the existence of distinct security features on the document. Presented identification documents – both official documents and those issued by other authorities and used to prove the link between a person and their claimed identity – are generally thoroughly scrutinized.

4.6.3. Social footprint as a means of identity verification

States that do not issue national identity cards are required to conduct in-depth verification of an individual's identity when issuing an identification document for use abroad, i.e., a travel document. Unlike in the case of countries that issue mandatory national identity cards, they cannot rely on information established and recorded for the issuance of identity cards.

Nevertheless, verification of breeder documents among source records is used wherever there is a direct online link. At the same time, this is not where the verifications end. To address the critical aspects of identification, i.e., to make sure that the identity belongs to a living person, that it is widely used in society and that it is linked to the applicant, other forms of identity documents issued by various government and non-government authorities are used to provide sufficient proof of identity. Depending on the country, other functional databases are consulted to make sure that the identity is in wide use and linked to the applicant, such as databases of issued driver's licences, and functional databases for various state-provided services may also be consulted for verification purposes. This is otherwise known as checking an applicant's **social footprint**.

The concept of a social footprint (not linked with social networks) assumes that a person, in their daily interactions with authorities and the private sector, leaves a trail whereby they use a specific identity, whether this is through enrolment in a school or university, employment, social services or use of a driver's licence. In many instances, information on an identity comes with other information, such as a photograph, that makes it possible to link a certain identity

with a specific person. The more such evidence can be obtained, the more the authorities can be assured that the identity exists, is in use and belongs to a specific person.

In the United States and the United Kingdom, travel document authorities outsource social footprint checks to commercial entities such as: CitzenSafe, Digidentity, Experian, the United States Postal Service, the Royal Mail, and SecureIdentity.

4.6.4. Verification of the link between an identity and a natural person for first-time applicants

After the authorities have verified that an identity exists and belongs to a living person, it is very important to establish that the identity belongs to the person applying for the document. Verification of the link to a specific claimed identity by adult applicants can be achieved through various approaches. The following is an overview of the methods used by some OSCE participating States, many being frequently applied across the OSCE area:

- An interview on the basis of the identity claims regarding the applicant, as well as their family;
- Witness statements or affidavits by individuals who are in a position to establish someone's facial identity (the fact that the personal data is truly associated with the person in the photograph) and who can be any person who has reached the age of majority, the director of an institution for children, the director of a general educational institution, the director of a medical institution, the head of administration of a prison/penitentiary establishment or the head of a military unit;
- In some instances, the police may be asked to conduct checks to verify that an identity belongs to the person claiming it; and
- Established practice in many states suggests that the link between an identity and a person has to be confirmed as part of the application process, if possible by at least two or more officials from the document issuing authority.

4.6.5. Collection of biometric identifiers

The collection of additional attributes, such as physical identifiers, is a critical aspect of the civil identification process. Biometric attributes represent distinctive, measurable physiological characteristics unique to an individual, e.g., facial features, fingerprints, voice, iris pattern, hand geometry and signatures. To a lesser extent, biometric attributes also include those characteristics that are not unique to an individual, but that serve to distinguish individuals, such as their age, sex, height, weight, eye colour and hair colour.

Before an identification document can be issued, physical identifiers are collected, recorded and linked with the identity being verified. The combined identity information and physical attributes are then introduced through a personalization process onto a secure medium for identification that is then used by the individual to facilitate their identification in their interaction with state and/or private entities.

As shown in Tables 4.9 and 4.10, a facial photograph is the main identifier collected, which is printed on the document and also stored in the database and linked with a specific identity. According to questionnaires completed by participating States, a digital signature is also often collected as a means of verification.

With the introduction of biometric passports, the collection of fingerprints also emerged as a desirable identifier in many cases, as they provide the fastest means of biometric identification using technology.

TABLE 4.9 BIOMETRIC INFORMATION ON NATIONAL IDENTITY CARDS ALSO STORED IN DATABASES OF ISSUED NATIONAL IDENTITY CARDS

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
What personal biometric information is stored in the database?	Digital photo	9	32	**31**	**97%**
	Digitized signature	9	32	**29**	**91%**
	Fingerprint	9	32	**13**	**41%**

TABLE 4.10 BIOMETRIC INFORMATION ON TRAVEL DOCUMENTS ALSO STORED IN DATABASES OF ISSUED TRAVEL DOCUMENTS

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
What personal biometric information on the travel document is also stored in the database?	Digital photo	4	37	**37**	**100%**
	Digitized signature	4	37	**32**	**86%**
	Fingerprint	4	37	**19**	**51%**

The collection of fingerprint information has so far been seen as very secure and easy to use for unambiguous identification, especially in cases where there is doubt in terms of matching other biometric identifiers on a document against the person presenting the document. Nonetheless, the issue of collecting fingerprint information has faced wide-ranging opposition. Opponents argue that a facial photograph should be sufficient for identification purposes, and that the collection of fingerprint information, despite its value in terms of secure biometric identification, presents a disproportionate intrusion into a person's privacy.

The debate on the value of collecting fingerprint information has resulted in varied practical implementation in terms of the collection, storage and use of fingerprint information. As Table 2.10 shows, only 51 per cent of participating States keep fingerprint information in their databases of issued passports. This percentage is even lower, 41 per cent, when it comes to keeping fingerprint information in a database (as shown in Table 4.9).

There are, however, fewer objections to collecting fingerprint information for storage and access on an identification document, provided that the information is not stored in a back-office database (Table 4.11 and Table 4.12).

TABLE 4.11 ELECTRONIC BIOMETRIC INFORMATION STORED ON NATIONAL IDENTITY CARDS

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Electronic biometric information stored on document:	No biometric information stored	9	32	**9**	**28%**
	Digital photo	9	32	**23**	**72%**
	Fingerprint	9	32	**12**	**38%**
	Digitized signature	9	32	**19**	**59%**

TABLE 4.12 ELECTRONIC BIOMETRIC INFORMATION STORED ON TRAVEL DOCUMENTS

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Electronic biometric information stored on travel document:	No biometric information stored	3	38	**0**	**0%**
	Digital photo	3	38	**38**	**100%**
	Fingerprint	3	38	**33**	**87%**
	Digitized signature	3	38	**26**	**68%**

Before biometric identifiers can be accepted as valid and linked with an applicant, authorities generally run automated queries in their database of collected biometric attributes to determine if another identity has already been established with the collected biometric sample. This is crucial to safeguard the principle of one record per person and a measure for identifying fraud attempts.

For this purpose, facial recognition systems and automated fingerprint identification systems are widely used.

Facial recognition system

A facial recognition system is a computer application that is capable of identifying or verifying a person's identity from a digital image. One of the ways it does this is by comparing selected facial features from an image and a database of faces. Facial recognition algorithms identify facial features by extracting landmarks, or features, from an image of the subject's face. For example, an algorithm may analyse the relative position, size and/or shape of the eyes, nose, cheekbones and jaw. These features are then used to search for other images with matching features.

Automated Fingerprint Identification System

The Automated Fingerprint Identification System (AFIS) is a biometric identification methodology that uses digital imaging technology to capture, store and analyse fingerprint data. The chief purpose of a civil fingerprint identification system is to prevent multiple records by conducting fingerprint matching in a database. The AFIS is a computerized storage system capable of searching tens of millions of fingerprint images. The database selects the most likely matches to any new print being fed into the system, thus narrowing the search parameters for investigators. Final analysis of the print and the retrieved images is carried out by AFIS technicians to ensure the accuracy of identification.

Table 4.13 presents an overview of the use of automated fingerprint identification systems and facial recognition systems across the OSCE region based on received responses from participating States. The table further shows the level of utilization of ICAO Checker, a software tool used for ensuring that the captured facial image meets relevant ICAO standards.

TABLE 4.13 USE OF SPECIAL TECHNOLOGIES FOR IMPROVED IDENTIFICATION AND DATA VERIFICATION PURPOSES

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses in proportion of received responses
Do you use any special technologies for improved identification and data verification purposes?	ICAO Checker	17	24	**13**	**54%**
	Facial Recognition System (FRS)	17	24	**9**	**38%**
	Automated Fingerprint Identification System (AFIS)	17	24	**7**	**29%**

4.7. IDENTITY AUTHENTICATION AS PART OF THE DOCUMENT RENEWAL PROCESS

When dealing with requests for renewal of identification documents, whether national identity cards or travel documents, the issuing authorities can benefit from the identity data collected and verified during the first and any subsequent applications for the document. In addition, the authorities can also access physical identifier information stored in the system.

In states where a national identity card is mandatory, when a person applies for a passport the issuing authorities benefit from the identity verification conducted as part of the process of issuing an identity card, which cuts down the lengthy process of verification needed for the issuance of the passport.

When applying for a document renewal, further supporting documentary evidence is usually not required provided that no changes have been made to the identity information compared to when the previous document was issued. If any identity information has changed (e.g., the applicant got married or changed their name), documentary evidence might be requested that is then verified in the source register (marriage register).

In countries that operate a population register, changes in identity information are constantly updated in the register, and any subsequent requests for the issuance of identity cards or travel documents can use only the information recorded in the population register. Any requests for changes in identity information must first be resolved in the population register before it can be reflected on identification documents.

In practice, identity information submitted in an application for document renewal is still verified further. This verification is carried out entirely by the issuing authority with no action required on the part of the applicant, except in cases where discrepancies occur in the verification process. The verification is completed by looking up the information in the database of issued national identity cards and/or passports. As Table 4.14 shows, most OSCE participating States have introduced processes for mandatory automatic and computerized identity data matching, as well as for matching biometric data against previously issued documents.

TABLE 4.14 TYPES OF IDENTITY VERIFICATION IN THE PROCESS OF RENEWAL OF IDENTIFICATION DOCUMENTS

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Automatic and mandatory online verification	Match between presented national identity card/travel document data and the data in the national identity card/ travel document database	0	41	**33**	**80%**
	Biometric match (photo match or fingerprint match)	0	41	**23**	**56%**
	Signature match against the signature on file	0	41	**7**	**17%**

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Mandatory verification in paper records	Match between presented national identity card/travel document data and the data in the national identity card/ travel document database	0	41	**8**	**20%**
	Biometric match (photo match or fingerprint match)	0	41	**3**	**7%**
	Signature match against the signature on file	0	41	**10**	**24%**

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Verification conducted only in case of doubt	Match between presented national identity card/travel document data and the data in national identity card/ travel document database	0	41	**5**	**12%**
	Biometric match (photo match or fingerprint)	0	41	**8**	**20%**
	Signature match against the signature on file	0	41	**13**	**32%**

A critical aspect of verification is linked with ensuring that the person submitting an application for document renewal is the same person to whom the previous document was issued. Verification can be carried out visually by the officials processing the application by comparing a photograph with the photograph already stored in the database. As the data provided reveals, authorities are increasingly relying on the use of technology to compare submitted photographs against photographs in their databases.

Where fingerprints are stored in a database, automated biometric fingerprint verification is also possible, by using automatic fingerprint identification systems. This option further extends to situations where a previously issued document stores fingerprint information but the information is not stored in a database. In this case, the applicant's identity is verified by comparing a fingerprint captured during submission of their application against the fingerprint data stored on the document.

Practice suggests that at least two points of verification of an applicant's identity and physical identifiers should exist, as well as independent review by two officials, especially if the automated verification in the database does not yield a positive result.

4.8. APPLICATIONS BY MAIL OR ONLINE

The practice in most OSCE participating States indicates that people can apply for a national identity card or travel document only by applying in person at designated application centres (Table 4.15). In some instances, however, some states also allow for remote application, including by applying online.

TABLE 4.15 REMOTE APPLICATIONS FOR NATIONAL IDENTITY CARDS AND/OR TRAVEL DOCUMENTS

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Do you allow applications for an identity card and/or passport by proxy or by applying online?	YES	0	41	**13**	**32%**
	NO	0	41	**28**	**68%**

For instance, where national identity cards are mandatory, applications for a passport can be submitted remotely, including as part of a first-time application, and the data used for the production of the passport can be taken from the information stored in the national identity card databases. In addition, the identity data is further verified by automatic verification in the civil registration record.

In some OSCE participating States, applications for passport renewal can be submitted by mail provided that specific supporting documentary evidence is provided and specific criteria met.

In the United States applications for passport renewal can be made as long as the undamaged (other than normal wear and tear) current passport is enclosed with the application, and the following conditions are met:

- The passport was issued when the person was age 16 or older;
- The passport was issued within the last 15 years;
- The passport was issued in the applicant's current name (or a name change should be documented with an original or certified copy of a marriage certificate, divorce decree or court order).

Good practice suggests that even if remote applications are allowed, additional verifications should be conducted to make sure that an application is not being submitted on behalf of a deceased person. In case of doubt, the applicant's social footprint may also be checked.

4.9. VERIFICATION IN OTHER DATABASES

Before a decision is made to issue an identification document, other information sources may be consulted that are not specifically linked directly with identity verification. This verification is mostly linked with situations where, due to specific circumstances, a document should not be issued. This is particularly relevant when it comes to issuing travel documents.

Authorities can maintain various so-called "lockout" databases that keep information that could provide the basis for denial of issuance of a travel document and/or an identity document.

There are various reasons why an application may be rejected. The database may return information that a valid identification document has already been issued or that a previously issued document was not returned or declared lost. There can also be a variety of legal obligations to be met and for which access to a document could be limited. For each basis for rejection, authorities normally operate databases or have access to such databases that should be consulted every time a new application for a document is submitted.

4.10. ADMINISTRATIVE ARRANGEMENTS FOR RETAINING INFORMATION ON ISSUED IDENTITY AND TRAVEL DOCUMENTS

Maintaining an archive of issued identification documents is an integral part of civil identification systems. The archive contains the information printed on identification documents, as well as documentary evidence accepted as legally valid proof of identity. This information from the archive is further used as a source of verification of issued identification documents including in the process of their renewal. As the information presented in Table 4.16 and Table 4.17 shows, digital databases have become the primary method for retention and management of collected personal information. Keeping paper archives remains a legal requirement in many participating States. Considering, however, that even in cases where paper archives still exist they are maintained in parallel with digital databases, it is clear that current systems rely more on digital than paper records. Tables 4.16 and 4.17 further show that, generally, almost all information printed on the identification document is also stored in a digital database.

In their completed questionnaires, the authorities of participating States also acknowledged that a wide range of other data normally not printed on the identification document is also stored in the database. These data originate from the documentary evidence submitted in support of applications for identification documents.

In many participating States authorities other than the civil registration authority are granted access to specific sets of data from civil identification records. Such access is granted in line with the national privacy protection legislation and in order to enable authorities access to up-to-date registered personal information or to allow them to verify the validity of presented identification documents in cases of doubt.

TABLE 4.16 INFORMATION PRINTED ON TRAVEL DOCUMENT ALSO STORED IN DIGITAL DATABASES

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Type of archive on issued travel documents?	Digital database	2	38	**38**	**100%**
	Paper archives	2	38	**16**	**42%**

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Is all personal information printed on the travel document also stored in the database?	YES	2	38	**36**	**95%**
	NO	2	38	**2**	**5%**

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
In addition to the travel documents issuing authority, do other national authorities have access to this information for verification purposes?	YES	2	38	**28**	**74%**
	NO	2	38	**10**	**26%**

TABLE 4.17 INFORMATION PRINTED ON NATIONAL IDENTITY CARDS ALSO STORED IN DIGITAL DATABASES

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Type of archive on issued identity cards?	Digital database	6	35	**35**	**100%**
	Paper archives (in addition to digital database)	6	35	**15**	**43%**

Responses by OSCE participating States		not response	response received	positive responses	% of positive responses as a proportion of received responses
Is all personal information printed on identity cards also stored in the database?	YES	6	35	**32**	**91%**
	NO	6	35	**3**	**9%**

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
In addition to the identity document issuing authority, do other national authorities have access to this information for verification purposes?	YES	7	34	**21**	**62%**
	NO	7	34	**12**	**35%**

Digital databases are also important instruments for inspection and resolution of issues linked with specific identities and identification data retained in the digital database. The experience of many authorities shows that despite strictly enforcing established procedures and making sure that all due diligence checks have been completed, a certain percentage of records and issued documents are categorised as problematic and require further monitoring and investigation. To address this situation, the authorities of some states have introduced a so called "traffic light system". Such a system requires inspection of civil registration records in the digital database. Those records considered safe are marked as "green", while records that raise some doubt as "yellow". Finally, those records that require mandatory follow up are marked as "red". These internal management marks provide guidance to the registration authorities in terms of the level of scrutiny required when dealing with the applications of certain individuals. Equally, other authorities with enabled access to civil identification databases can be alerted if they are dealing with an individual for whom civil registration authorities would advise further verification.

4.11. CIVIL IDENTIFICATION FOR RESIDENT NON-CITIZENS

Freer movement and greater mobility is the reality of the OSCE region. People cross borders in search of better job opportunities and better prospects for the well-being of their families. In the European Union (EU), for instance, the free movement of people, including for the purposes of resettling in another country, is one of the foundation principles around which the EU was built. In reality, depending on the state, the total number of resident non-citizens may represent a sizable proportion of the total population.

As the status of resident non-citizens enables people to access a wide range of entitlements, most importantly to remain on the territory of the state they are living in, the authorities responsible for identity management need to work closely with migration authorities to ensure that resident non-citizens are provided with an identification document that they can use as proof of their status and to access specific services provided by the state. Such identification documents have different official titles that depend on the country that issues the document. For instance, EU countries issue two types of identification cards for resident non-citizens: permanent resident cards (for citizens of other EU states) and long-term residence permits (for citizens of non-EU states). Eurostat data from 2016 revealed that there were 20.7 million people residing in an EU member state who were citizens of a non-member country on 1 January 2016, representing 4.1 per cent of the entire EU population. In addition, there were 16 million people living in EU Member States on 1 January 2016 who were citizens of another EU member state.

In absolute terms, the largest numbers of non-citizens living in EU member states on 1 January 2016 were found in Germany (8.7 million), the United Kingdom (5.6 million), Italy (5 million), Spain (4.4 million) and France (4.4 million). Non-nationals in these five Member States collectively represented 76 per cent of the total number of non-nationals living in all of the EU member states, while the same five member states had a 63 per cent share of the EU's total population. More precise information on the proportion of resident non-citizens in the total population of EU Member States is provided in Table 4.18.[5]

5 Non-national population by group of citizenship, 1 January 2016, Eurostat website, <http://ec.europa.eu/eurostat/statistics-explained/index.php/File:Non-national_population_by_group_of_citizenship,_1_January_2016_(%C2%B9).png>.

TABLE 4.18 PROPORTION OF RESIDENT NON-CITIZENS IN THE TOTAL POPULATION OF EU MEMBER STATES AS OF 1 JANUARY 2016

	Total		Citizens of another EU Member State		Citizens of a non-member country		Stateless	
	(thousands)	(% of the population)	(thousands)	(% of the population)	(thousands)	(% of the population)	(thousands)	(% of the population)
Belgium	1 327.4	11.7	875.9	7.7	450.8	4.0	0.7	0.0
Bulgaria	73.8	1.0	13.1	0.2	58.8	0.8	f.9	0.0
Czech Republic	476.3	4.5	195.4	1.9	280.9	2.7	0.0	0.0
Denmark	463.1	8.1	189.4	3.3	267.2	4.7	6.5	0.1
Germany	865.2	10.5	380.1	4.6	4 840.7	5.9	10.3	0.0
Estonia	197.6	15	15.4	1.2	1 823	13.9	0.0	0.0
Ireland	586.8	12.4	3 840	8.1	2 011	4.3	1.6	0.0
Greece	798.4	7.4	206.7	1.9	591.7	5.5	0.0	0.0
Spain	4 418.2	9.5	1 934.3	4.2	2 483	5.3	0.9	0.0
France	4 408.6	6.6	1 529.1	2.3	28 794	43	0.0	0.0
Croatia	40.9	1.0	13.5	0.3	26.7	0.6	0.8	0.0
Italy	5 026.2	8.3	151.7	2.5	3 508.4	5.8	0.7	0.0
Cyprus	139.6	16.5	109.1	12.9	30.5	3.6	0.0	0.0
Latvia	288.9	14.7	6.0	0.3	282.8	14.4	0.2	0.0
Lithuania	18.7	0.6	4.9	0.2	12.3	0.4	1.4	0.0
Luxembourg	269.2	46.7	229.5	39.8	39.6	6.9	0.1	0.0
Hungary	156.4	1.6	85.1	0.9	71.1	0.7	0.2	0.0
Malta	30.9	7.1	15.5	3.6	15.4	3.5	0.0	0.0
Netherlands	834.8	4.9	458.7	2.7	367.7	2.2	8.3:	0.0
Austria	1 249.4	14.4	615.6	7.1	629.8	7.2	4.0	0.0
Poland	149.6	0.4	25.1	0.1	1 239	3.0	0.6	0.0
Portugal	388.7	3.8	105.2	1.0	283.5	2.7	0.0	0.0
Romania	107.2	0.5	48.0	0.2	58.9	0.3	0.3	0.0
Slovenia	107.8	5.2	17.6	0.9	90.2	4.4	0.0	0.0
Slovakia	65.8	1.2	50.4	0.9	13.9	0.3	1.5	0.0
Finland	228.2	4.2	94.2	1.7	133.1	2.4	0.9	0.0
Sweden	773.2	7.8	304.0	3.1	447.7	4.5	21.6	0.2
United Kingdom	5 640.7	8.6	3 204.6	4.9	2 436.0	3.7	0.0	0.0
Iceland	26.5	8.0	21.8	6.6	4.5	1.4	0.1	0.0
Liechtenstein	12.8	34.0	6.7	17.8	6.1	16.2	0.0	0.0
Norway	534.3	10.3	341.7	6.6	190.2	3.6	2.4	0.0
Switzerland	2 047.2	24.6	1 357.6	16.3	689.3	8.3	0.3	0.0

Unlike temporary visitors, foreigners who wish to stay permanently on the territory of a destination state need to apply for permanent resident status. After this status has been confirmed by the relevant authorities, it is further certified by issuing identification documents in the format of a residence card.

Identity information established as part of the granting of residence status is used for the production and personalization of residence cards. Identity information is verified against the presented travel document issued by the authorities of the country the applicant is a citizen of. In case of doubt, further checks in terms of whether the document provided is genuine or not may be conducted, often in consultation with border authorities, who can use specialized forensic equipment for this purpose.

To help guide the verification of foreign-issued travel and/or identification documents, authorities benefit from services tailored to provide information on the layout and security features of travel and other identification documents issued by the authorities of recognized states. As indicated in Table 4.19, OSCE participating States reported using the PRADO and EDISON TD services most frequently. These services provide information that is publicly available, as well as more precise information on documents with restricted access only for registered state authorities.

PRADO – The Council of the European Union **P**ublic **R**egister of **A**uthentic Travel and Identity **D**ocuments **O**nline

http://www.consilium.europa.eu/prado/en/prado-start-page.html

PRADO contains technical descriptions, including information on some of the most important security features of identity and travel documents of countries within the European Union, all Schengen Area countries, of other neighbouring countries, as well as of many non-EU countries worldwide.

With Council Joint Action 98/700/JHA of 3 December 1998, the European Image Archiving System **FADO** (***F****alse and* ***A****uthentic* ***D****ocuments* ***O****nline*) was set up. The first part of the system, Expert FADO, went online at the end of 2004 for secure communication among document experts. In 2007, iFADO and PRADO were released. ***iFADO*** (*intranetFADO*) contains the most important information from Expert FADO for access restricted to governmental use, while in PRADO a small subset of this information is published for the general public.

PRADO contains basic technical descriptions, including information on security features, of authentic identity and travel documents. The information is selected and provided by document experts in the Member States of the European Union, Iceland, Norway and Switzer land; part of the information contained in the classified, restricted Expert FADO system is made publicly available via the PRADO pages.

EdisonTD (TD is an abbreviation of 'travel documents') is a database that contains information about travel and travel-related documents from almost every country in the world. The database was developed by the Dutch authorities in close co-operation with the authorities in Australia, Canada, the United Arab Emirates and the United States of America, as well as Interpol.

The content is available in Arabic, Dutch, English, French, German and Spanish.

EdisonTD's verification level is freely available on the Internet at the following address: http://www.edisontd.net/.

DISCS users have automatic access to EdisonTD's control level, which has more images and information available than EdisonTD's verification level.

TABLE 4.19 PUBLIC AND/OR COMMERCIAL REGISTERS USED FOR VERIFICATION OF THE AUTHENTICITY OF FOREIGN-ISSUED DOCUMENTS

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Which public and/or commercial registers are used for verification of the authenticity of foreign travel and identity documents?	PRADO	17	24	**22**	**92%**
	EDISONTD database	17	24	**4**	**17%**

Other than identity information, authorities also collect biometric identifiers that are included on identification documents and also recorded in a database to facilitate subsequent verification of issued identification cards.

Responses received from participating States indicate that, in many cases, in addition to a facial photograph, fingerprint information is also collected and recorded. As shown in Table 4.20, fingerprint information is recorded almost as often as facial photographs. This also means that, in many participating States where citizens are not required to provide their fingerprint information, this requirement is not waived for resident non-citizens.

TABLE 4.20 COLLECTION OF UNIQUE IDENTIFIERS OF RESIDENT NON-CITIZENS

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Unique identification number assigned to resident foreign nationals	YES	8	33	**25**	**76%**
	NO	8	33	**8**	**24%**

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Do you require resident foreign nationals to provide fingerprints at some point during their stay or upon entry?	YES	8	33	**27**	**82%**
	NO	8	33	**6**	**18%**

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Are the photos of all foreigners, regardless of their legal status, kept for the identification purposes?	YES	7	34	**29**	**85%**
	NO	7	34	**5**	**15%**

5. RISK ANALYSIS

The purpose of developing identity management infrastructure is to enable people, citizens primarily, to exercise their rights and to benefit from certain entitlements. Identity management processes are therefore designed to facilitate civil registration and identification of a large majority of the population who need identification documents for legitimate purposes.

There are, however, people who, for various reasons, try to obtain services to which they are not entitled. As access to rights and entitlements normally requires that a person present valid identity documents, these documents are a central subject of interest among people who wish to access services to which they are not entitled. Even though they may not be entitled to certain rights and services, they will try to obtain identity documents – either genuine or falsified – that will grant them such access. This demand is often coupled with the supply of false documents that could be used undetected by criminal groups that exploit gaps in identity management infrastructure.

The most severe consequences can emerge in situations where an individual is able to obtain falsified or genuine identity documents under a fraudulent identity to conceal their true identity, which they then use in the commission of criminal acts of varying degrees, including terrorist acts.

5.1. INHERENT WEAKNESSES OF CIVIL REGISTRATION SYSTEMS

Civil registration can certify that a certain identity exists, but it is not designed to certify links between identities and specific people. The use of information technology has resulted in improvements in the way that civil registers are being operated and information collected, processed and retained, as well as in improvements in the security of the management of identity data and, to a certain degree, has helped address security gaps in identity management that threaten the very integrity of the register.

5.1.1. Lack of a link between identity information and a natural person

Civil registers do not collect, process or store biometric information (such as photographs, fingerprints, etc.) during the registration of vital life events. It has been scientifically proven that commonly used biometric identifiers (fingerprints primarily) are unreliable up to a certain age. To bridge this gap in identity management, most OSCE participating States issue mandatory identity cards where, at the point of issuance (in a procedure described in greater detail in the section on civil identification), a link is created and registered between the identity data from the civil register and a physical person through collection of a photograph and, in some cases, fingerprints. By requiring the issuance of identification documents, it is possible to correlate identity data with a specific person for a large percentage of the population. In many OSCE participating States that operate population registers, a photograph is also stored in the register, thereby becoming permanently associated with a specific identity.

Even with the mandatory issuance of national identity cards, the idea that the entire population should have an official identification document has, however, never been completely fulfilled, as there are numerous identities in a civil register of people who have not reached the age where possession of a national identity card is mandatory. The emerging security gap in the safe identification of the underage population is being addressed by requesting that parents or legal guardians linked with a specific identity identify themselves with a national identity card.

In some OSCE participating States, such as the United States and Canada, national identity cards are not issued, and some other form of identification document might be required to verify the link between an identity and the person claiming that identity. The criteria may vary, however, depending on the type of services requested. Generally, the highest level of scrutiny is reserved for the issuance of passports.

While civil registration is of great importance for civil identification as it provides breeder documents on the basis of which identification documents can be issued, civil identification is equally important for maintaining the integrity of the civil registration system.

In the process of the registration of vital life events, the identity of the person requesting registration is determined by checking the information printed in their official identification documents. For instance, during the registration of a birth, which introduces a new identity that is also linked to the newborn's parental information, the parents' identity information in many OSCE participating States is verified by checking officially issued identification documents.

Another security gap emerges from the fact that, among the adult population, there can be many people whose information is in the civil register but who have, for whatever reason, left the country to live permanently abroad and therefore never obtained an identification document. When not duly addressed, this creates a pool of identities for which there is no information linking them with a physical person. This pool could be utilized for fraudulent purposes, such as linking an existing identity with a different person.

5.1.2. Security of civil registration certificates

In most OSCE participating States, certificates issued from the civil register are not secure documents. There are no international standards, as in the case of travel documents, to dictate the design and security features of civil registration certificates. Consequently, civil registration certificates in the OSCE region, even in cases where security features have been introduced in the document, are no match for the type of security offered in the design and production of travel documents and in many cases of national identity cards. At the same time, civil registration documents and birth certificates in particular are the primary proof of identity used to acquire a very secure travel document or a national identity card.

This lack of security has led to an inherent flaw in all processes of identity management, where civil registration documents as proof of identity are the weakest link in the process of issuing national identity cards and travel documents.

Most breeder documents are much easier to forge than e-passports, and by using forged breeder documents (via identity theft or a fake national identity card), genuine travel documents can be obtained.

ORIGINS Project

The EU has commissioned specific projects aimed at addressing the identity management security gap emerging from non-standard birth certificates and the lack of a physical identifier on certificates. The first such project, called Fidelity, resulted in a range of recommendations, including the introduction of a standard birth certificate design to be used in all EU member states. Building on the research conducted as part of the Fidelity project, the EU also supported a consortium of private and state actors, as well as academia, as part of the ORIGINS project, established to investigate security gaps in passport breeder documents, mainly birth certificates. The aim of the project is to recommend possible solutions enabling more secure and efficient authentication of individuals at passport issuing points, which will indirectly improve the reliability of border control activities, while at the same time protecting the privacy of citizens through a privacy-by-design approach. The aim of ORIGINS is to propose cost-effective solutions to dramatically improve the security of the process of issuing breeder documents.

In many OSCE participating States, the problem of the lack of security of registration certificates is mitigated by creating preconditions that enable verification of the identity data from a certificate directly in the source database. Such verification can be carried out by remote access to the population or central civil register depending on the type of register operated. In participating States where only local civil registers are digitized, verification is carried out by enabling online access to the database at the local registry office that issued the certificate in question. This good practice is elaborated on in greater detail in the section on identification documents.

5.2. CIVIL IDENTIFICATION FRAUD

When it comes to civil identification fraud, the following classifications can be applied:

- **Counterfeit document:** a document that constitutes an unauthorized reproduction of a genuine document. Such documents are not legitimately manufactured, nor are they issued or recognized by an official authority;
- **Forged documents:** these are typically based on a genuine document, a part of which has been added or altered in order to provide misleading information about the person presenting it;
- **Blank stolen documents:** blank authentic documents that were misappropriated and personalized by an unauthorized person or entity;
- **Fraudulently obtained documents** (with and without internal help): an authentic identity or travel document obtained through deception by submission of either false or counterfeit documents, co-operation of a corrupt official or impersonation of the rightful holder of a genuine document;
- **Imposters:** misuse of a genuine document through deception by a person who knowingly misrepresents themselves by using someone else's identity or travel document. Often, the biographical details and photograph resemble the impostor, helping them pass as the rightful bearer; and
- **Pseudo documents:** documents produced with no authority and that are not officially recognized. They can be found in various forms and may have the physical appearance of a passport or a national identity card.

Ongoing improvement in the security of identification documents is very important and is the best instrument for fighting all but two categories of identity fraud: fraudulently obtained documents and blank stolen documents. Making documents secure and difficult to counterfeit or alter has, for many years, been the most challenging aspect in terms of maintaining the credibility of national frameworks for civil identification. Achievements made in this area have also meant that the attention being paid to identity deception has shifted from the actual documents to the issuing process and systems for identity management.

All listed categories of identity fraud (except fraudulently obtained documents) deal with interventions involving alterations of identification documents, whether the document is fabricated or genuine. Fraudulently obtained documents, on the other hand, can be obtained only if there are gaps in the identity management process.

Essential to identification management are measures that are free of any gaps that can facilitate document and/or identity fraud during the issuing process. Fraud cases that have been examined after they were detected by chance have shown that it is possible to commit fraud due to gaps in the process or solutions that have not been fully thought through. Sometimes, it is the result of human error or an intentional action on the part of officials.

Good practices and the general design of processes dealing with applications for identification documents or registration of vital life events described in this Compendium are developed with the intention of detecting and preventing attempts to fraudulently obtain documents. While most applications are genuine, the more services and entitlements a document provides, the more the system is likely to face increased attempts to fraudulently obtain such documents.

These attempts can be categorized in the following groups:

- Creating a fictitious identity:
  - Individuals who intentionally provide misleading personal information to the issuing authority in order to create a new identity, e.g., their date of birth or name or surname; and
  - Individuals using counterfeit documents, like passports, identity cards, birth certificates, driver's licences, etc. to obtain a genuine document based on a false identity.

- Altering one's own identity by changing one or more elements of one's attributed identity (identity manipulation):
  - Individuals who intentionally provide misleading personal information to the issuing authority as part of their own identity, e.g., their date of birth or name or surname; and
  - Individuals who provide inconsistent identity information during the application process to different issuing authorities in order to collect multiple identities and receive several identity documents based on different personal information.

- Stealing or assuming an identity with or without consent (identity theft/imposture), often of a deceased individual:
  - Category 1 imposters are individuals who try to use someone else's personal information to obtain a genuine identity card or passport; and
  - Category 2 imposters are individuals who use someone else's identity document and who have a reasonable resemblance to the person on the photograph in the document, thereby obtaining a genuine identity card or passport.

- Stealing or assuming an identity, which is subsequently manipulated, e.g., stealing an identity and then changing the date of birth to reflect the imposter's actual age:
  - Individuals using counterfeit documents, e.g., passports, identity cards, birth certificates, family books, driver's licences, to obtain a genuine document based on a false identity; and
  - Individuals using altered or falsified documents to obtain a genuine document based on the personal information in those documents.

These represent typical examples of attempts to fraudulently obtain documents. Once such documents have been issued, they are very difficult to detect, as they enjoy the same status as any other authentic document. Identity management is being carefully scrutinised to find new gaps that can be exploited. Elaborate schemes have been identified that are aimed at defeating identity managements systems, as in the following examples:

- Fake birth declarations create identities for future use. This type of fraud can be used by criminal organizations. Members of the organization declare the birth of a child who is never actually born. Proof of birth is issued, and this official document is given to the criminal organization. In 18 years' time, this identity can be given to a member of the organization, who can then apply for a travel document, since this identity has never been used by anyone else. This modus operandi depends heavily on how a state's birth registration process is organized.

- Three-in-one identities. In such situations, a fraudster uses three different parts of an identity to complete one full identity. The main aim is to conceal their full identity while still being able to use the fake identity. The modus operandi is that the fraudster uses a fake name or a name from an existing person; then, a photograph with a pretty good resemblance but not that of the fraudster is submitted; finally, the fraudster has to be enrolled in the biometric system. For this, they have to use their own fingerprints. Only the fingerprints are from the fraudster, and the other two parts are from someone else. It is even possible that the

fraudster will use a thin film over their fingers that contains an impression of the fingerprints of someone else, who will then be registered. In this situation, no real identity information from the fraudster will be available.

- Learning of an identity registered in civil registration records that is not in wide use and exploiting that identity by obtaining genuine civil registration breeder documents and subsequently acquiring a genuine identity document. This can happen in a situation where a person moves abroad and is likely not to return soon or if a person dies abroad, but that information never reaches the civil registration authorities.

5.2.1. Document issuance and control

The primary purpose of an identity management system is to issue trusted and trustworthy identity documents that will enable the bearer to access rights and benefits and also enable public-sector entities to efficiently provide these rights and benefits.

Identity management does not end with the completion of the application process and entitlement decisions. A decision in terms of entitlement to an identification document based on a completed application review and concluded identity verification will eventually result in the inclusion of correct information in the database of issued identification documents. Practice shows, however, that security gaps linked with the human factor, mainly as a consequence of corrupt staff, could result in identification documents issued to individuals who did not pass all verification checks. A similar result can also be achieved by enabling access to blank identification documents and personalization facilities.

To mitigate these risks, good practice suggests that issuing authorities systematically assess the processes and protocols for document issuance, looking specifically into:

- Application processes;
- Entitlement processes;
- Treatment of materials and blank books;
- Personalization and delivery;
- Document security;
- Facility security;
- Information technology security; and
- Personnel and internal integrity.

The ICAO "Guide for Assessing Security of Handling and Issuance of Travel Documents"6 outlines key steps authorities need to take to complete an assessment and provides recommendations for closing specific security gaps linked with the issuance of identification documents.

6 ICAO, "Guide for Assessing Security of Handling and Issuance of Travel Documents", <https://www.icao.int/Security/mrtd/Downloads/Guidance%20Material/Part%203%20-%20A%20Guide%20for%20Experts.pdf>.

TABLE 5.1 INTERNAL AUDITS OF REGISTRATION AND VETTING OF REGISTRATION STAFF

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Do you conduct audits of document issuance processes to ensure the integrity of the data entry/verification process?	NO	1	40	**14**	**35%**
	YES	1	40	**26**	**65%**

Responses by OSCE participating States		no response	response received	positive responses	% of positive responses as a proportion of received responses
Do you conduct staff vetting and periodic checks of staff involved in the documents issuance process concerning their credit rating, debt levels, financial commitments, etc.?	NO	2	39	**23**	**59%**
	YES	2	39	**16**	**41%**

The practice of many OSCE participating States, as shown in Table 5.1, suggests that there is a need to conduct systematic security checks on employees who, due to personal financial problems or other reasons, may be corrupted and who may then exploit access to identity databases, blank documents or personalization equipment. Such checks can be conducted by looking into unusual processing and searches conducted in databases storing personal identification information that may point to attempts at fabricating identities. The practice of many participating States shows that some of the most serious breaches of the identity management framework are not the result of flaws in procedures, but rather the result of corruption on the part of the issuing authorities.

ANNEX 1. OSCE COMMITMENTS AND INTERNATIONAL STANDARDS

Identity management: OSCE commitments and priorities

ODIHR's involvement with population registration derives from the commitment by participating States to "[...] their common determination to build democratic societies based on [...] the rule of law", as stated in the Preamble and Paragraph 2 of the 1990 OSCE Copenhagen Document. Two key areas of the Office's work – democratic elections and freedom of movement – are vital to the implementation of this commitment.

In addition to the 1990 OSCE Copenhagen Document, important provisions of international law are also relevant to population registration. The Preamble to the United Nations' International Covenant on Civil and Political Rights (ICCPR) states that "the ideal of free human beings enjoying civil and political freedom and freedom from fear and want can only be achieved if conditions are created whereby everyone may enjoy his civil and political rights, as well as his economic, social and cultural rights".

Neither the 1990 OSCE Copenhagen Document nor the ICCPR specifies the legal or administrative frameworks that states should adopt in order to meet these obligations and commitments. Population registration and identity management systems are not the subject of specific OSCE commitments. They are, however, a means of achieving the implementation of fundamental commitments and international standards in three distinct areas: the rule of law, the right to vote and the freedom of movement (particularly in respect of the choice of place of residence).

The basis for national legislation is often found in international conventions. A number of articles in such conventions may be applicable for a particular national law. This is also the case for the registration and management of identities of human beings. Hereunder, the reader will find a number of international conventions and their specific articles that are related to identity management in general and to the registration of birth, national identity cards or passport laws and the right to travel.

Universal Declaration of Human Rights (UDHR), 10 December 1948

Article 6: Everyone has the right to recognition everywhere as a person before the law.

Article 13: (1) Everyone has the right to freedom of movement and residence within the border of each state.
(2) Everyone has the right to leave any country, including his own and return to his country.

Article: 15: (1) Everyone has the right to a nationality.
(2) No one shall be arbitrarily deprived of his nationality nor denied the right to change nationality.

Convention of the Rights of the Child, 20 November 1989

Article 7: (1) The child shall be registered immediately after birth and shall have the right from birth to a name, the right to acquire a nationality and, as far as possible, the right to know and be cared for by his or her parents.
(2) States Parties shall ensure the implementation of these rights in accordance with their national law and their obligation under the relevant international instruments in this field, in particular where the child would be otherwise stateless.

Article 8: (1) States Parties undertake to respect the right of the child to preserve his or her identity, including nationality, name and family relations as recognized by law without unlawful interference.
(2) Where a child is illegally deprived of some or all of the elements of his or her identity, States Parties shall provide appropriate assistance and protection, with a view to re-establishing speedily his or her identity.

The International Covenant on Civil and Political Rights, 23 March 1976

Article 12: (1) Everyone lawfully within the territory of a State shall, within that territory, have the right to liberty of movement and freedom to choose his residence.
(2) Everyone shall be free to leave a country, including his own.
(3) The above-mentioned rights shall not be subject to any restrictions except those which are provided by law, are necessary to protect national security, public order (ordre public), public health or morals or the rights and freedom of others, and are consistent with the other rights recognized in the present Covenant.
(4) No one shall be arbitrarily deprived of the right to enter his own country.

There are a number of articles in the ICCPR that are also covered in other international conventions. For example, Article 16 is the equivalent of Article 6 of the UDHR, while Article 24(2) and (3) is the equivalent of Article 7 of the Convention on the Rights of Child.

Convention Relating to the Status of Refugees, 28 July 1951

Article 27: The Contracting States shall issue identity papers to any refugee in their territory who does not possess a valid travel document.

Article 28: (1) The Contracting States shall issue to refugees lawfully staying in their territory travel documents for the purpose of travel outside their territory, unless compelling reasons of national security or public order otherwise require, and the provisions of the Schedule to this Convention shall apply with respect to such document.
The Contracting States may issue such a travel document to any other refugee in their territory; they shall in particular give sympathetic consideration to the issue of such a travel document to refugees in their territory who are unable to obtain a travel document from the country of their lawful residence.

(2) Travel documents issued to refugees under previous international agreements by parties thereto shall be recognized and treated by Contracting States in the same way as if they had been issued pursuant to this article.

Convention Relating to the Status of Stateless Persons, 28 September 1954

Article 27: The Contracting States shall issue identity papers to any stateless person in their territory who does not possess a valid travel document.

Article 28: (1) The Contracting States shall issue to stateless persons lawfully staying in their territory travel documents for the purpose of travel outside their territory, unless compelling reasons of national security or public order otherwise require, and the provisions of the Schedule to this Convention shall apply with respect to such document.

The Contracting States may issue such a travel document to any other stateless person in their territory; they shall in particular give sympathetic consideration to the issue of such a travel document to stateless persons in their territory who are unable to obtain a travel document from the country of their lawful residence.

ANNEX 2. GUIDANCE MATERIALS FROM THE UNITED NATIONS STATISTICS DIVISION

As part of its work, the United Nations Statistics Division issued the Principles and Recommendations for a Vital Statistics System, Revision 3, which was adopted by the Statistics Commission at its forty-fifth session in 2014. The original principles and recommendations for a vital statistics system, Principles for a Vital Statistics System: Recommendations for the Improvement and Standardisation of Vital Statistics, were adopted by the Statistical Commission in 1953 and were primarily designed as guidelines for countries whose vital statistics were already based on a civil registration system or that were planning to adopt such a system.

Revision 3 is a guide for national governments for establishing and maintaining reliable civil registration systems for legal documentation on events throughout the lifetime of individuals like birth, changes in marital status and death. It provides technical guidance on standards, concepts, definitions and classifications for civil registration and vital statistics to further increase international comparability of data. It takes developments in technology and computing into account that can greatly enhance civil registration. Principles and Recommendations for a Vital Statistics System are accompanied by *Handbooks on Civil Registration and Vital Statistics Systems each providing specific procedural recommendations for the effective design and operation of the various aspects of effective civil registration and vital statistics systems:*

- *Handbook on Civil Registration and Vital Statistics Systems: Management, Operation and Maintenance* (1998): this Handbook provides guidance to countries for the improvement of their civil registration and vital statistics systems, as well as background and specifications for developing and establishing civil registration and vital statistics systems in countries that do not yet have such systems in place. The Handbook deals with essential components of the structure, management, operation and maintenance functions to handle the entire range of vital events – live births, deaths, foetal deaths, marriages and dissolutions of marriage – from the civil registration and the vital statistics perspectives. It also covers forms, data collection, record processing, storing and editing of information, issues of security, the issuing of certificates, the functional relations between the civil registration system and the vital statistics system, the legal and administrative requirements and the daily operational and maintenance activities to ensure completeness, timeliness and accuracy.

- *Handbook on Civil Registration and Vital Statistics Systems: Preparation of a Legal Framework* (1998): this Handbook shows how to develop a comprehensive legal framework for a civil registration system that supports its juridical function, its role as a source of continuous

vital statistics and its use by other agencies such as health ministries, electoral rolls, identification services, population registers and pension funds, which depend on accurate registration data. The Handbook will assist country experts in preparing a civil registration law to conduct complete, accurate and timely registration of vital events (live births, foetal deaths, marriages, divorces, legal separations, annulments of marriage, deaths, adoptions, legitimations, recognitions).

- *Handbook on Civil Registration and Vital Statistics Systems: Developing Information Communication* (1998): this Handbook provides guidance to countries in designing and conducting information, education and communication activities to support national civil registration and vital statistics systems. It covers the development of a communication action plan for community workshops and meetings and for communication with the media, as well as special techniques to reach target groups and less privileged populations and those who live in rural areas. It also discusses resource mobilization, development of a time frame, required resources and identification and mobilization of human resources.

- *Handbook on Civil Registration and Vital Statistics Systems: Policies and Protocols for the Release and Archiving of Individual Records (1998): this Handbook is a comprehensive guide for countries for designing policies on the confidentiality of individual information on vital records and on adjunct statistical forms. It also offers methods to permanently store and protect vital records.*

- *Handbook on Training in Civil Registration and Vital Statistics Systems (2002): this Handbook provides guidance for developing a national capability to operate and maintain, in a co-ordinated manner, the fundamental systems of civil registration and vital statistics. It contains course material, consisting of 23 modules that can be adapted to conduct effective and comprehensive training on the essentials of civil registration and vital statistics systems. The modules address a range of issues related to the establishment, operation and maintenance of reliable civil registration and vital statistics systems.*

- *Handbook on Civil Registration and Vital Statistics Systems: Computerization (1998): this Handbook provides guidance to national authorities for the development of data processing systems for civil registration and vital statistics systems. It focuses on advance planning for computerization and proposes options for countries to consider, including organizational structures for computerization. It examines the framework, goals and purposes of computerization of civil registration; looks at the interfaces between civil registration, the vital statistics system and other governmental agencies; and enumerates some of the major decisions and problem areas that should be anticipated.*

- *Handbook of Vital Statistics Systems and Methods, Vol. I, Legal, Organizational and Technical Aspects, and Vol. II, Review of National Practices: this Handbook supersedes the Handbook of Vital Statistics Methods published by the United Nations in 1955. It provides up-to-date guidance to countries for implementing international recommendations adopted by the United Nations on vital statistics systems. Volume I addresses issues emerging in running and co-ordinating comprehensive civil registration and vital statistics systems and their co-ordination. Volume II, published in 1985, reviews national practices in civil registration and vital statistics systems and methods.*

ANNEX 3. GUIDANCE MATERIALS FROM THE INTERNATIONAL CIVIL AVIATION ORGANIZATION

The **International Civil Aviation Organization** (ICAO) is a specialized UN agency, established by states in 1944 to manage the administration and governance of the Convention on International Civil Aviation (Chicago Convention).

The ICAO works with the Convention's 191 states parties and industry groups to reach consensus on international civil aviation standards and recommended practices (SARPs) and policies in support of a safe, efficient, secure, economically sustainable and environmentally responsible civil aviation sector. These SARPs and policies are used by ICAO member states to ensure that their domestic civil aviation operations and regulations conform to global norms, which in turn permits more than 100 000 daily flights in the aviation's global network to operate safely and reliably in every region of the world.

At the 38th session of the ICAO Assembly (24 September – 4 October 2013), member states adopted the ICAO Traveller Identification Programme (ICAO TRIP) Strategy. TRIP aims to establish the goals and objectives of traveller identification management, to lead and reinforce a global approach and to provide direction for action by the ICAO, states and the many international, regional and industry partners in identification management.

TRIP consists of the following five key elements:

1. **Evidence of identity:** credible evidence of identity, involving the tracing, linkage and verification of an identity against breeder documents to ensure the authenticity of the identity;

2. **Machine-readable travel documents (MRTDs):** the design and manufacture of standardized MRTDs, including e-passports, that comply with ICAO specifications;

3. **Document issuance and control:** processes and protocols for document issuance by appropriate authorities to authorized holders, and controls to prevent theft, tampering and loss;

4. **Inspection systems and tools:** inspection systems and tools for the efficient and secure reading and verification of MRTDs, including the use of the ICAO PKD; and

5. **Interoperable applications:** globally interoperable applications and protocols that provide for timely, secure and reliable linkage of MRTDs and their holders to available and relevant data in the course of inspection operations.

Under key element 2, MRTDs, the ICAO sets the standards and specifications for the development of all MRTDs like passports and electronic passports, diplomatic passports, identity cards, etc. These standards are laid down in Document 9303, Machine Readable Travel Documents, Seventh Edition, 2015. This document includes a total of 12 parts. Each part explains a specific topic related to the development of an MRTD. Hereunder follows a short explanation of the content of all the different parts.

Part 1: Introduction – The content of this part informs readers about general considerations like relative costs and benefits of MRTDs, operations and endorsement by the ISO. Other topics are related to definitions and references and, finally, guidance on the use of Document 9303 is provided.

Part 2: Specifications for the Security of the Design, Manufacture and Issuance of MRTDs – This part covers important topics like the security of MRTD production and issuance facilities, the provision of information on lost and stolen MRTDs and the sharing of information with INTERPOL, security standards for MRTDs that explain which security features should be incorporated in an MRTD and which personalization technique could be used. Furthermore, recommendations are given about machine-assisted document security verification covering machine authentication of security features and advice that readers can use for that purpose.

Part 3: Specifications Common to All MRTDs – These specifications cover all three formats of documents described in Document 9303, namely TD1 (credit card size), TD2 (identity card size) and TD3 (passport size). Topics discussed include which information can be stored in the visual inspection zone and how the machine-readable zone is organized; codes for nationality, place of birth and location of issuing state/authority; and recommendations for transliteration and examples of how to calculate check digits.

Part 4: Specifications for Machine Readable Passports (MRPs) and Other TD3-Size MRTDs – The construction and dimensions of an MRP and MRP data page are explained, as is the general layout of the MRP data page. Examples of a personalized MRP data page are also shown.

Part 5: Specifications for TD1-Size Machine-Readable Official Travel Documents (MROTDs) – This part is important when a state would like to introduce a TD1-size identity card. Topics described include the dimensions of a TD1-size MROTD, the general layout and contents of a TD1-size MROTD, such as the visual inspection zone and machine-readable zone. Technical specifications for a machine-readable crew member certificate are also explained.

Part 6: Specifications for TD2-Size Machine-Readable Official Travel Documents (MROTDs) – This part is important when a state would like to introduce a TD2-size identity card. Topics described include the dimensions of a TD2-size MROTD, the general layout and contents of a TD2-size MROTD, such as the visual inspection zone and machine-readable zone.

Part 7: Machine-Readable Visas (MRVs) – If a state decides to develop a visa sticker, the first choice they have to make is if it should be an MRV-A or MRV-B. Both visa types are described in this part, as are the layout and the technical specifications. Furthermore, there is a possibility to add a barcode to the visa sticker, and models of the different types are shown. Another important aspect is explained on how to position the visa sticker in a passport or other machine-readable document. Part 7 is currently under revision, and a new version will be published in due time.

Part 8: Reserved for future use – It is foreseen that the first item that will fall under this category will be specifications for emergency travel documents.

Part 9: Deployment of Biometric Identification and Electronic Storage of Data in e-MRTDs – States that are considering introducing an electronic passport or other travel document should first read this part to get a general understanding of how to develop an e-passport. Items covered include: the chip-inside symbol, the validity period for e-MRTDs, a warning regarding care in handling e-MRTDs and information about biometric verification and storage of the information in a contactless chip. This part is an important guide for senior managers and project managers on the complex implementation of e-passports.

Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in a Contactless Integrated Circuit (IC) – This part is for IT specialists who will develop the LDS on the contactless chip. It covers the requirements for the LDS, the application profile, the file structure, the elementary files and the data elements forming data groups 1 through 16.

Part 11: Security Mechanisms for MRTDs – This part describes the digital security of the chip and its content. Different mechanisms are described, such as how to get access to the chip, authentication of data (passive authentication), authentication of the contactless chip (active chip authentication), as well as other access control mechanisms (extended access control).

Part 12: Public Key Infrastructure – This part is a very important component of the overall security of e-MRTDs. It is meant for the IT specialists who are tasked with developing the national public key infrastructure (PKI). It covers the requirements for issuing states and topics such as roles and responsibilities, key management, distribution mechanisms, PKI trust and validation.

Owing to the ICAO's recommendations, requirements and specifications, every state today complies with these standards, which have created a truly globally interoperable system for reading and verifying passports at international borders. This is a significant contribution to global security, and it facilitates immigration processes at airports, as well as at land and sea borders. Adding biometric features, like facial images, fingerprints or iris scans, to the contactless chip in machine-readable passports shows that the level of security has grown substantially. It is now up to the border management agencies worldwide to upgrade their infrastructure to be able to read these features and use them in their border systems to verify the identity of bearers.

ANNEX 4. OSCE IDENTITY MANAGEMENT QUESTIONNAIRE

Survey questionnaire

COMPENDIUM OF GOOD PRACTICES IN IDENTITY MANAGEMENT

Information
This questionnaire was prepared by the OSCE Office for Democratic Institutions and Human Rights (ODIHR) in partnership with the OSCE Transnational Threats Department / Action against Terrorism Unit (TNTD/ATU) as part of an on-going activity related to the development of a "Compendium of Good Practices on Identity Management". The objective of this activity is to support OSCE participating States in implementing OSCE commitments on freedom of movement and travel document security. The compendium is being developed with a view to improving practice and strengthening knowledge among authorities in participating States on secure identity management and the issuance of travel documents.

Your support and information is critical to the success of this project, and we thank you in advance for your co-operation!

Target Audience
We recommend that the questionnaire be completed by the national authority responsible for the issuance of travel and identity documents.

Objective
This Compendium will serve as a reference guide on good practice procedures for the issuance of travel documents based on the integrity and verifiable evidence of identity. Working in partnership with the TNTD ATU, ODIHR will take stock of existing policies on identity management and use of evidence of identity as part of travel documents issuance process, identifying and promoting good practices through the publication across the OSCE region. Identification and promotion of good practices in this area will help authorities in OSCE participating States to review and potentially adjust and improve their existing national policies, contributing to improved identity management and more secure cross-border travel in the OSCE region.

This questionnaire is designed to collect information on the national systems of identity management in OSCE participating States. It was designed with an assumption that every national identity management system is unique and has been developed according to national interests and needs taking into account national tradition and culture. Therefore, certain practices in identity management may only be useful and applicable to specific contexts and countries. Consequently, the compendium to be developed, based on the information received through this questionnaire, will not be used to rank or assess systems either as good or bad; rather, it aims at revealing good approaches in identity management that help prevent identity fraud with the view to sharing this information for consideration by identity management practitioners in OSCE participating States. Additionally, information received through this questionnaire will be valuable in terms of updating information on existing systems to recognize new trends and approaches in identity management.

Requests for clarification

Please send your completed questionnaires in electronic (Microsoft Word) format **by 9 September 2016** directly to Mr. Zoran Dokovic, OSCE ODIHR Adviser on Migration, Freedom of Movement and Human Contacts (Zoran.Dokovic@odihr.pl) and Mr. Simon Deignan, Programme Manager – Travel Document Security, TNTD/ATU (simon.deignan@osce.org). In the event that respondents have difficulty in the completion of this questionnaire, require additional details or have questions, they should be directed to Zoran Dokovic at OSCE ODIHR (Zoran.Dokovic@odihr.pl, +48 603 638 999).

Country	
Completed by:	Name:
	Institution:
Contact e-mail:	
Telephone:	
Date:	

Identity document (ID card)		
Document issuing authority		
Authority responsible for document printing/ personalization		☐ State owned entity ☐ Contracted vendor

Information printed on ID card

☐ First Name ☐ Family Name ☐ Date of Birth ☐ Address ☐ Sex
☐ Date of issue ☐ Personal Number ☐ ID Number ☐ Expiry date ☐ Photo
List other information:

Does the ID have personal data encoded in machine readable zone: ☐ YES ☐ NO

Is the ID design fully comply with ICAO standards ☐ YES ☐ NO Limited compliance

Electronic biometric information stored on document:		**What type of chip is used on the card (if used):**
No biometric information stored	☐	☐ Contact based ☐ Contactless ☐ Dual interface
Digital photo	☐	
Fingerprint – add how many (☐☐)	☐	
Digitized signature	☐	
Type of archive on issued ID cards?		☐ Digital database ☐ Paper archives

Please fill out only in case the information is retained in database

Is *all* personal information printed on ID card also stored in the database? ☐ YES ☐ NO

If NO please list information not stored:

Please list personal information stored in the database but not printed on the ID (if applicable):

What biometric personal information stored in the database?
☐ Digital photo ☐ Digitized Signature ☐ Fingerprint (how many fingers ☐☐)

Further to ID issuing authority do other national authorities have access to this information for verification purposes ☐ YES ☐ NO
If YES please list for which type of services:

Travel document (passport)		
Document issuing authority		
Authority responsible for document printing/ personalization		☐ State owned entity ☐ Contracted vendor

Information printed on ID card

☐ First Name ☐ Family Name ☐ Date of Birth ☐ Address ☐ Sex
☐ Date of issue ☐ Personal Number ☐ ID Number ☐ Expiry date ☐ Photo
List other information:

Electronic biometric information stored on the document:		**What type of chip is used on the passport (if used):**
No biometric inform ation stored	☐	☐ Passive Authentication (PA) ☐ Basic Access Control (BAC) ☐ Extended Access ☐ Control (EAC) ☐ Supplemental Access ☐ Control (SAC)
Digital photo	☐	
Fingerprint – add how many (☐☐)	☐	
Digitized signature	☐	
Type of archive on issued passports?		☐ Digital database ☐ Paper archives

Please fill out only in case the information is retained in database

Is *all* personal information printed on the passport also stored in the database? ☐ YES ☐ NO

If NO please list information not stored:

Please list personal information stored in the database but not printed on the passport (if applicable):

What biometric personal information stored in the database?
☐ Digital photo ☐ Digitized Signature ☐ Fingerprint (how many fingers ☐☐)

Further to ID issuing authority do other national authorities have access to this information for verification purposes ☐ YES ☐ NO
If YES please list for which type of services:

Establishing/verifying identity during application for travel and/or identity document

Please describe the process of verifying identity for a person applying for identity or travel document for the first time (where no record of previously issued ID/passport exist).
Please list supporting documentary evidence required:

In case of children, is the presence of mother, father or both parents/legal guardians required?
☐ YES ☐ NO

Please describe the methodology used to verify that documentary evidence submitted matches the person applying for the document for the first time:

Please, describe separately the process of verifying identity for a person applying for identity or travel document where one of the two documents has already been issued in the past.
Please, list required supporting documentary evidence:

Do you allow application for ID and/or passport by proxy or by applying online? ☐ YES ☐ NO
If YES, please describe under what conditions such applications are allowed:

Do you verify independently and ex-officio with the issuing authorities relevant information submitted through documentary evidence:
☐ Verified only during first issuance
☐ Verified during first and all subsequent issuance
☐ Verified only in case of doubt in legitimacy of submitted documents

Please mark applicable means of conducting verification of identity data from the application against relevant databases/ registers:	**Automatic and mandatory on-line verification**	**Mandatory verification in paper records**	**Verification conducted only in case of doubt**
Match between presented ID/travel document data and the data in ID/travel document database	☐	☐	☐
Biometric match (photo match or fingerprint)	☐	☐	☐
Signature match against deposited signature	☐	☐	☐
Civil register (birth records)	☐	☐	☐
Civil register (deceased persons)	☐	☐	☐
Civil register (marriage records)	☐	☐	☐

Is there a unique identifier or personal identification number (PIN) assigned to each person?
☐ YES ☐ NO

If YES, the PIN is defined as: ☐ Random number ☐ Logical construct

At what point of time is the identifier is assigned to an individual?
☐ At birth (entered in the civil register) ☐ Upon first issuance of ID/travel document

Is the same unique identifier used by other government services for keeping personal information in their databases? ☐ YES ☐ NO

If NO, please indicate the type of information other institutions use to uniquely identify individuals:

If applicable, what is your assessment of other national institutions' verification of data printed on the ID against the electronic information stored on ID chip?
☐ Not conducted ☐ Conducted rarely ☐ Conducted frequently ☐ Such checks are mandatory

If applicable, what is your assessment of other national institutions' verification of data printed on the passport against the electronic information stored on the passport chip?
☐ Not conducted ☐ Conducted rarely ☐ Conducted frequently ☐ Such checks are mandatory

Do you use any special technologies for improved identification and data verification purposes?
☐ ICAO Checker*
* Computer software used to ensure that data generated for storage (including biometric data such is photo) can be read by other systems, or similarly, that a system can read the data from any standards-compliant passport.
☐ Face Recognition System (FRS)
☐ Automated Fingerprint Identification System (AFIS)
Other (please list):

Internal control mechanisms
In which format do you retain supporting documentary evidence for applications for travel and identity documents: *(Please list all which apply)* ☐ Digital database containing scanned images of the documents ☐ Digital database with data entered according to separate fields of the supporting document ☐ Paper archive
Do you conduct audits of document issuance processes to ensure integrity of data entry/verification process: ☐ YES ☐ NO **If YES, what type, objectives and frequency of these audits:**
Do you conduct staff vetting and periodic checks on staff involved in the documents issuance process concerning their credit rating, debt levels, financial commitments etc? ☐ YES ☐ NO If **YES**, how often:
List relevant machine/software based validations embedded in the system aimed at preventing human error and/or fraudulent attempts to obtain documents:

Foreign nationals entitled to residence document
List types of documents issued to resident foreign nationals (excluding foreign diplomatic corps) **:**
Is there any unique identifier assigned to resident foreign nationals either specifically designed for them or a national identifier assigned specially for resident foreigners? ☐ YES ☐ NO
Do you require resident foreign nationals to provide fingerprints at some point during their stay or upon entry? ☐ YES ☐ NO If **YES**, list states whose nationals are exempted from this requirement:
Are the photos of all foreigners regardless of their legal status kept for the identification purposes? ☐ YES ☐ NO
Which public and/or commercial registers are being used for verification of authenticity of foreign travel and identity documents? ☐ PRADO – Public Register of Authentic travel and identity Documents Online ☐ EDISONTD database Other:
When dealing with the documents issued by foreign authorities, what other mechanisms are being used in order to verify the authenticity and correctness of data?

Civil Status Registration

Which authority (ies) is/are in charge of registering civil status and issuing corresponding certificates or documents?

Which of the following best describes your system of civil status registration?

☐ **Event-based**
In an event-based registration system in its pure form, each event that has an effect on the civil status of a person is recorded at the place where the event occurred. The birth of a person is recorded at the place of birth. Marriage is recorded at the place of marriage. A divorce is not recorded at all, since divorces take place in courts and not under the authority of the civil status registrars. A person who wishes to marry and who has been married before, needs to state so and present the former marriage certificate and the divorce decree for evidence, even within the same state.

☐ **Person-based**
In a person-based system, an entry for every person born in that jurisdiction is made at one particular place. All subsequent changes to the civil status of that person, all changes of name, marriages, divorces, children and, eventually, the death of that person, are registered at that same place. In some jurisdictions, this may be a national central registry. In the absence of a central database, a decision needs to be made as to the place of a person's registry. In some jurisdictions, it is the place of birth. However, since the place of birth can be random, it is often the place of the family's residence or the place of the family's inherited domicile.

☐ **Central population register**
In a population register, all citizens and permanent residents have an entry in the system linked to a personal identification number ("PIN"). With respect to civil status, it is, of course, a person-based system. But as opposed to the person-based civil registration system described as above, the entries in the population register are not restricted to matters of civil status and related issues. Rather, a population register records many other items of information, such as residence, employment, taxes, driver's license and social benefits. While civil status certificates may be issued, these are no longer really necessary. Whenever information is required that was traditionally provided via a certificate, the authority could usually obtain that information on-line and directly out of the system.

Is the archive related to the civil status registration digitized?
☐ YES ☐ NO ☐ Partially
If Partially, approximately what percentage is digitized?

What is the approach used for digitization?
☐ Stored image filled of a registration act
☐ Document data entered according to separate fields of the registration act
☐ An image file of an original document also attached? (to control for possible data entry errors)
☐ Only key data entered according to separate fields of the document instead of digitizing every single data
☐ Is an image file of an original document also attached? (to control for possible data entry errors)

Legislation

Please attach specific internal regulations, secondary law, training manuals, internal instructions developed with the view to prevent identity fraud in the process of application for identity and travel documents?
These documents can be provided as attachments in the email and/or as web links for download.

ANNEX 5. GLOSSARY

Authentication
(a) The process of establishing confidence in the truth of a claim, which could be any declarative statement. (b) The process by which a user conveys data into a system in order to be recognized and to be able to interact with the system. (c) In biometrics, sometimes used as a generic synonym for certification.

Biometrics
A measurable physical characteristic or personal behavioural trait used to recognize the identity or verify the claimed identity of an individual, such as the facial image, fingerprints, gait or iris.

Blank stolen documents
Blank authentic documents that were misappropriated and personalized by an unauthorized person or entity.

Breeder document
An identification document issued to support a person's identity and used to obtain another document or privilege of greater perceived value, such as a passport or driver's license. The most important breeder document is the birth certificate.

Civil identification
The verification, registration, management, and conservation of personal data of citizens, with the goal of establishing a unique civil identity. Civil identification includes all of the data from the civil registration on that particular citizen as well as other attributes such as a unique number and/or biometric data. The civil identification serves as a basis for the verification of identity (i.e., passport or national identification documents).

Civil register
The repository of loose-leaf file, ledger book, electronic file, or any other official file set up for the universal, continuous and permanent recording, in accordance with established procedures, of each type of vital event and its associated data of the population of a defined area (e.g., county, district, municipality or parish).

Civil registration system
The institutional, legal, and technical norms established by government to conduct civil registration in a technical, sound, co-ordinated and standardized manner throughout the country, taking into account cultural and social circumstances particular to the country.

Counterfeit document
A document that constitutes an unauthorized reproduction of a genuine document. Such documents are not legitimately manufactured, nor are they issued or recognized by an official authority.

Forged document
Typically based on a genuine document, a part of which has been added or altered in order to provide misleading information about the person presenting it.

Fraudulently obtained document
An authentic identity or travel document obtained through deception by submission of either false or counterfeit documents, co-operation of a corrupt official or impersonation of the rightful holder of a genuine document.

Identity management
A combination of systems, rules and procedures that are defined between an individual and organizations regarding the entitlement, use and protection of personal information in order to authenticate individual identities and provide authorization and privileges within or across systems and enterprise boundaries.

Identity management
A set of policies, practices and protocols for managing the identity and trust of information technology users and devices across organizations.

Identity theft
The illegal acquisition of confidential information so that unauthorized individuals can use it to impersonate the true owner of the identity.

Imposter
A person who knowingly misrepresents themselves by using someone else's identity or travel document. Often, the biographical details and photograph resemble the impostor, helping them pass as the rightful bearer.

Legalization of documents
A written official declaration by a competent authority certifying the authenticity of a signature in a public or private act, providing validity to it wherever submitted.

Machine-readable travel document (MRTD)
An international travel document that contains some information readable by humans and other information readable only by machine. All MRTDs include the holder's identification details, including picture or digital image, with compulsory identification elements included in a device-readable zone.

Personalization
The process by which a person's data is included on a substrate that will become an identity or travel document.

Population register
An individualized data system, i.e., a mechanism for continuous recording and/or co-ordinated linkage of selected information pertaining to each member of a country's resident population that makes it possible to provide up-to-date information about the size and the characteristics of the population. Thus, it is the result of a continuous process in which notifications of certain events, recorded originally in different administrative systems, are automatically and instantly used to update the population register on an ongoing basis.

Primary identity documents
Documents issued for the purpose of establishing an individual's legal identity. (see also secondary and tertiary identity documents)

Pseudo documents
Documents produced with no authority and that are not officially recognized. They can be found in various forms and may have the physical appearance of a passport or a national identity card.

Public policies for identity management
Policies that cover government actions that aim to reformulate and update existing legal administrative models. The goal is to transform and incorporate technological innovations to improve the service of identity authentication, building a positive relationship with citizens through a guaranteed universal ability to exercise one's right to a legal identity and management based on transparency and accountability in institutions.

Secondary identity documents
Secondary identity documents enable access to certain rights and privileges and are

issued only on the basis of the presentation of a primary identity document (e.g., student ID) (see primary identity documents).

Social footprint check
The process of consulting functional databases to make sure that the identity is in wide use and linked to the applicant, such as databases of issued driver's licenses, and functional databases for various state-provided services may also be consulted for verification purposes.

Statelessness
The condition of not being considered a national by any state under the operation of its laws.

Tertiary identity document
Documents that enable specific entitlements (e.g., health service card) (see primary identity documents).

The International Civil Aviation Organization (ICAO)
A specialized UN agency, established by states in 1944 to manage the administration and governance of the Convention on International Civil Aviation (Chicago Convention) that works with the Convention's 191 states parties and industry groups to reach consensus on international civil aviation standards and recommended practices (SARPs) and policies in support of a safe, efficient, secure, economically sustainable and environmentally responsible civil aviation sector.

Unique identification number
A unique identification number assigned to each identity in the system, to ensure unique and unambiguous searches for a specific identity, reinforcing the principle of one record per person.

Vital event record
A legal document entered in a civil register that attests to the occurrence and characteristics of a vital event (a live birth, death, foetal death, marriage, divorce, adoption, legitimation, recognition of parenthood, annulment of marriage, or legal separation).

Vital statistical record
A document or record that contains those items of information concerning an individual vital event.

Vital statistics system
The total process of (a) collecting information by civil registration or enumeration on the frequency of specified and defined vital events, as well as the relevant characteristics of the events themselves and of the person(s) concerned, and (b) compiling, processing, analyzing, evaluating, presenting and disseminating these data in statistical form.