



FREE MOVEMENT ZONES: GUIDE FOR ISSUANCE AND BORDER MANAGEMENT

The opinions expressed in the report are those of the authors and do not necessarily reflect the views of the International Organization for Migration (IOM). The designations employed and the presentation of material throughout the report do not imply the expression of any opinion whatsoever on the part of IOM concerning the legal status of any country, territory, city or area, or of its authorities, or concerning its frontiers or boundaries.

IOM is committed to the principle that humane and orderly migration benefits migrants and society. As an intergovernmental organization, IOM acts with its partners in the international community to: assist in meeting the operational challenges of migration; advance understanding of migration issues; encourage social and economic development through migration; and uphold the human dignity and well-being of migrants.

Publisher

International Organization for Migration
17 route des Morillons
P.O. Box 17
1211 Geneva 19, Switzerland
Tel.: +41 22 717 9111
Fax: +41 22 798 6150
Email: hq@iom.int
Website: www.iom.int

Authors

Stephan D. Hofstetter
Rajeshkumar Raja

Coordination & Collaboration

Nelson Gonçalves (IOM)
Niall McCann (UNDP)

The development of this guide was funded by
the People of Japan



Developed under the supervision of:



This publication has issued without formal editing by IOM.

© 2021 International Organization for Migration (IOM)

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior written permission of the publisher

FREE MOVEMENT ZONES: GUIDE FOR ISSUANCE AND BORDER MANAGEMENT


Foreword

Ensuring legal identity for all is at the heart of facilitating safe, regular and orderly cross-border mobility and migration. Legal identity is a critical enabler of global mobility and central to the protection of migrants' rights throughout their journeys and upon arrival. The inability to present proof of legal identity has a detrimental effect on migrants, starting from their inability to exercise their right to leave and return to their country, and extending into integration into their host societies and access to rights and services. It can also be a major impediment to enter another territory. Well-managed migration contributes directly to the 2030 Agenda for Sustainable Development and its central commitment to leave no one behind.

This publication emanates from the work and discussions within the UN Legal Identity Agenda Task Force (UNLIA TF). The Task Force counts 15 UN agency members and was established in 2018 with the aim to actively support UN Member States to develop comprehensive birth-to-death civil registration and legal identity systems. In addition to traditional civil registration and the issuance of certificates such as birth and marriage certificates, many Member States have also rolled out national ID programmes in recent decades. Within some regional groups (such as the EU), these national ID cards can be used as travel documents within the agreed free movement zone. However, contrary to passports, where common technical standards have been developed under the auspices of the International Civil Aviation Organization, national ID documents so far do not have such a common set of internationally recognized technical standards. The Task Force therefore decided to develop this guide, via the leadership of the International Organization for Migration, in order to provide best practice guidance to Member States when developing national ID document schemes that can be used for international travel.

In 2020, the number of international migrants reached 281 million, despite the impact of the Covid-19 pandemic, which is projected to reduce the growth in the stock of international migrants by around 2 million (DESA, 2021). Migrants have been severely affected by the travel restrictions and lockdowns implemented during the COVID-19 pandemic, while also playing a critical role in pandemic response, particularly as essential frontline workers.

This reference document is part of IOM's activities centered around the implementation of the UN Legal Identity Agenda Task Force Annual Workplan, which UNDP co-chairs alongside UNICEF and UNDESA. With the increased use and recognition of ID cards for international travel, we hope this publication will serve as useful guidance for national and international policy makers and practitioners, ultimately contributing to better and more secure border control, and most importantly, to the facilitation of safe travel for migrants.

Ugochi Daniels 
Deputy Director General
for Operations
IOM

 **Haoliang Xu**
UN Assistant Secretary-General
Director of the Bureau for
Policy and Programme Support
UNDP

TOPICS

TABLE OF CONTENTS	7
INTRODUCTION	11
PART I: GETTING STARTED	19
Chapter 1: What are Free Movement Zones	21
Chapter 2: What are the reasons to establish FMZs? And why not?	29
Chapter 3: What do you need to consider when establishing FMZs?	37
Chapter 4: Examples of FMZ initiatives	41
PART II: BUILDING CONSENSUS ON INTERGOVERNMENTAL LEVEL	49
Chapter 5: Getting started	51
Chapter 6: What topics need to be handled	61
PART III: DESIGNING THE CREDENTIALS	73
Chapter 7: Selecting the credentials for FMZ travels	75
Chapter 8: Designing the credentials	101
Chapter 9: Non-Physical credentials	121
PART IV: DESIGNING AN ADEQUATE BORDER MANAGEMENT	125
Chapter 10: Managing traveller experiences	127
Chapter 11: Document verification	129
Chapter 12: Automated Border Crossings	143
Chapter 13: Biometrics for border management	153
ANNEX 1: SOME TECHNOLOGICAL FUNDAMENTALS	155
Chapter 14: PKI and the chip in travel documents	157
Chapter 15: Biometrics	171
Chapter 16: Linking of identities with people	175
Chapter 17: UPINs – Considerations on harmonization	179
ANNEX 2: ACRONYMS AND MORE	183

TABLE OF CONTENTS

INTRODUCTION	11
1. About this guide	12
2. How to use this guide	16
3. Icons used in this guide	17
4. Interaction and future work	18
PART I: GETTING STARTED	19
Chapter 1: What are Free Movement Zones	21
5. What is meant by 'Free Movement'	22
6. What are the different types of existing travel arrangements	24
7. Definition of FMZ for the sake of this guide	27
Chapter 2: What are the reasons to establish FMZs? And why not?	29
8. Political considerations	30
9. Economic considerations	31
10. Social considerations	32
11. Security considerations	33
12. Who benefits and loses from this free movement	34
Chapter 3: What do you need to consider when establishing FMZs?	37
13. Are there pre-requisites for establishing an FMZ	38
Chapter 4: Examples of FMZ initiatives	41
14. European Union	42
15. Common Travel Area (UK, Ireland)	43
16. Oceania	44
17. Caribbean Community (CARICOM)	45
18. Southern Common Market (Mercosur/sul)	46
19. Common Market for Eastern and Southern Africa (COMESA)	47
20. East African Community (EAC)	47
21. Economic Community of West African States (ECOWAS)	47

PART II: BUILDING CONSENSUS ON INTERGOVERNMENTAL LEVEL 49

Chapter 5: Getting started 51

- 22. What are our priorities 52
- 23. How do you find a minimal common interest and anticipate blocking points 54
- 24. Establishing political will and operational engagement 55
- 25. What are key areas for harmonization 58

Chapter 6: What topics need to be handled 61

- 26. For which user groups 62
- 27. Common visa policy 63
- 28. Common border management policy 64
- 29. Intelligence and data exchange 65
- 30. Granted rights 66
- 31. Leadership and ongoing monitoring 67
- 32. Which ports/border-crossings are to be considered 67
- 33. Establishment of citizenship 68
- 34. Dispute resolution 69
- 35. Decision on interoperability and use of standards 70

PART III: DESIGNING THE CREDENTIALS 73

Chapter 7: Selecting the credentials for FMZ travels 75

- 36. Which credentials could be considered for FMZ travels 76
- 37. Considerations on place of issuance and personalization 80
- 38. Considerations for eMRTD issuance and personalization 83
- 39. Considerations for the personalization technology 84
- 40. Considerations of the document material 87
- 41. Considerations for data storage 91
- 42. Functional considerations for selecting the document 96

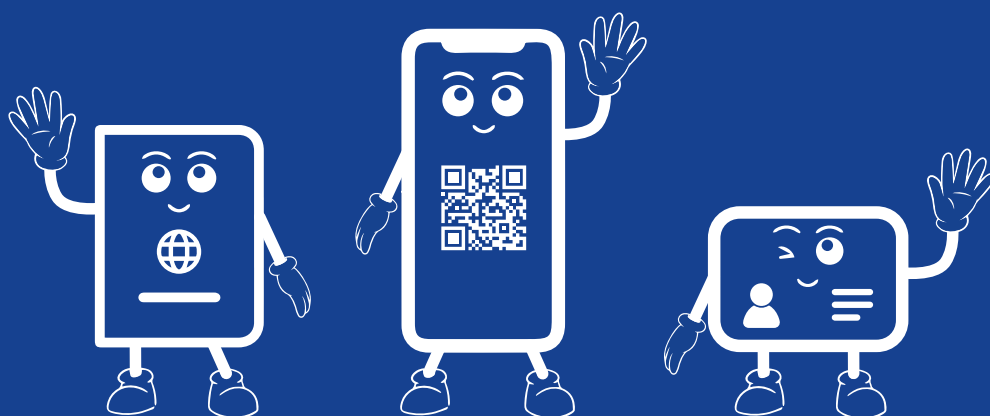
Chapter 8: Designing the credentials 101

- 43. Getting started when designing the FMZ credential 102
- 44. How do we design a harmonized security concept 103
- 45. Harmonized visual data-layouts 109
- 46. Decisions on access control for eMRTDs 113
- 47. Access control for biometrics 114
- 48. Considerations for biometric capture 115
- 49. Considering special needs 116
- 50. Where can I find out more about this subject 116

Chapter 9: Non-Physical credentials	121
51. What are forms of non-physical credentials	122
52. Considerations when contemplating the introduction of non-physical credentials	122
53. Where can I find out more about what is going on in this field	124
PART IV: DESIGNING AN ADEQUATE BORDER MANAGEMENT	125
Chapter 10: Managing traveller experiences	127
54. Options for traveller management at the borders	128
Chapter 11: Document verification	129
55. Procedures for document verification of official travel documents	130
56. How are eMRTDs verified	133
57. Preconditions for successful eMRTD verification	135
58. Does ePassport verification always give a yes/no answer	137
59. How to manage Automated Border Crossing	139
60. Guidance for document verification of non-passport documents	139
61. Where can I get additional information on the subject	141
Chapter 12: Automated Border Crossings	143
62. What are Primary Inspection Kiosk machines (PIK)	144
63. What are eGates	145
64. What can eGates do	147
65. What if something goes wrong, and how can we know	148
66. What are the prerequisites for a proper use of ABC-Terminals	150
Chapter 13: Biometrics for border management	153
67. What is the role of biometrics in border management	154
68. What to consider when using biometrics on the borders	154
ANNEX 1: SOME TECHNOLOGICAL FUNDAMENTALS	155
Chapter 14: PKI and the Chip in travel documents	157
69. What are some core concepts of cryptography	158
70. Applying the concepts to protect a message	162

71. How is PKI used in eMRTDS	166
72. The contents of the chip	168
Chapter 15: Biometrics	171
73. A brief introduction to biometric identification	172
74. Types of Biometrics used in travel documents	173
Chapter 16: Linking of identities with people	175
75. Evidence of Identity	176
76. How to make sure that people don't acquire multiple identities	178
Chapter 17: UPINs - Considerations on harmonization	179
77. What are UPINs	180
78. Is there a need for a uniform, inter-operable UPIN for the region	181
ANNEX 2 - ACRONYMS AND MORE	183
79. Acronyms and Glossary	184
80. Stakeholders	188
81. Tables	190
82. Figures	190

INTRODUCTION



1. About this guide

“ You look at where you’re going and where you are and it never makes sense, but then you look back at where you’ve been and a pattern seems to emerge. ”

- Robert M. Pirsig, *Zen and the Art of Motorcycle Maintenance: An Inquiry Into Values*.

BACKGROUND

The UN Legal Identity Agenda supports the implementation of the strategic development goals (SDG) target 16.9, “legal identity for all, including birth registration, by 2030.” The aim of the current project is to explore ways to standardise cross-border identity document systems, both regionally and globally, to facilitate easier international travel and migration. Extensive documentation, manuals, guides and training materials have been developed in the past. Most of them are very ‘issuer-centric’, and with a particular (technical) vocabulary and focus. They offer little benefit for the practitioner in border management.

CURRENT STATUS

Issuance of identity credentials as part of a national identity management scheme, such as national ID cards, are a sovereign right, and since such ID documents are generally issued for use within that country, their harmonization across economies has not been considered necessary in the past. Some countries, however, have followed ICAO Doc 9303 in designing their national ID documents, and this has already led to a degree of harmonization across multiple countries. However, due to national regulations/requirements, there has been an element of ‘localization’ in the design of these ID documents. This may or may not lead to interoperability issues, and these have not been studied in much detail until now.

Without some degree of harmonization of identity documents, the challenge of validation/authenticating them is immense. This can lead to a subversion of the system by bad actors, which would negatively impact the Free Movement Zones. Having said that, a degree of localization must be allowed as countries have different internal needs for identity documents within their own borders. So, an ideal approach would be to

specify a minimum set of standards that should be followed, and allow for specific country features.

Too much standardization and harmonization, however, could be a double-edged sword. For example, Doc 9303 suggests some security features but does not mandate any of them. This is intentional. If every national ID card producer in the world had identical security features, then a single compromise would lead to compromise of all travel documents. Similarly, for embedded chips within eMRTDs, minimum cryptographic algorithms are specified, with a wide divergence being allowed for the same reasons. A high level of standardization can lead to smaller attack surfaces for fraudsters, however. Compromising a single feature can compromise the entire system.

A key consideration is the legal framework within which identity documents are issued. These have developed over time and at different speeds and may impact on how much standardization or harmonization is possible. Most countries insist on data minimization for documents that are presented for verification overseas, while allowing more information-rich data sets for documents used in country.

With respect to Free Movement Zones, there are two possible scenarios: a) a borderless system, as exists in the Schengen Area, which functions as a single jurisdiction for international travel purposes, with a common visa policy and which is, by definition, 'borderless', and b) a "visa free travel" without any restrictions model, such as the one being considered in regional groupings in Africa.

It was planned to develop a user-centric guide for issuing authorities and verifiers of identity documents (e.g. border control authorities) taking into account existing standards and procedures with consideration of continental and regional specifics.

The research methodology entailed study of legal and policy documents on existing cross border document system standardization initiatives. Secondary data from existing research papers in the area of Free Movement Zones was also considered.

MANDATE

METHODOLOGY
AND FINDINGS

The desk research threw up some expected findings.

1. There are quite a few well written research papers that cover the legal, economic and security aspects of the free movement of people. They are a factual analysis of the current state of affairs and include the extent to which the reality matches the intended goals.
2. Many initiatives for free movement of people exist, but almost all of them can best be described as a 'work in progress'.

The validation of the research was done through semi-structured interviews with representative participants in free movement schemes. One of the questions asked was about their opinion on the contents of this guide. A few common themes emerged during these discussions.

1. The legal basis for free movement of persons was pretty much well understood and established. Almost all the people involved in the process are fully conversant with existing legal frameworks and their associated adequacies or inadequacies.
2. Lessons were learnt as the scheme progressed and modifications have been done based on these lessons. It would have been good if these points had been considered at the origination of the project. For example, entry/exit systems in case there is a common border around a free movement area.
3. The starting point was different for different schemes. For example, Mercosur was established to enable accelerated development through co-operation. The African Union developed out of the Organisation of African Unity with a number of continental cohesion goals, one of which was establishing a cohesive identity. The establishment of the EU was focused on reduction of conflict etc. The initial participants in the process had a

clear vision of where they wanted to reach and as long as they were part of the process, significant development was achieved. However, currently, most of the people involved are focused on the details and it would be good to step back and look at the bigger picture.

4. Identity documents pretty much follow ICAO Doc 9303 specifications, but there also exist a plethora of identity documents that do not follow any standard. It was commonly recognized that the ultimate aim is to follow ICAO specifications and that these specifications were comprehensive and sufficient. No new harmonization was required or aimed specifically at standards or specifications for regional travel documents.
5. It would be good if a summary document detailing the points to consider when establishing Free Movement Zones was available.
6. While technical personnel at operational level understand the specifications, a simpler introduction to the specifications for people involved in policy decisions would be welcome.
7. Border control is usually not part of the conversation when ID documents are specified and a simple guide for them to understand the complexities of eMRTDs would be helpful.

As a result of the conversations with practitioners in the area of free movement of people, it was decided to tackle three themes in this guide.

- Theme A: A compilation of the areas that need to be covered when considering free movement of people. No evidence of such a document on this topic could be found at present. While there may be people who are perhaps eminently more qualified than the authors to cover this topic, they felt that a document that lists

various aspects to consider in the process of setting up free movement of people is necessary.

- Theme B: A short introduction to the different technological aspects of issuing of credentials that are in conformance with the Doc 9303 specifications. These could be with an ID card common design or a passport.
- Theme C: An overview of the technical aspects of identity credentials from the viewpoint of a border control practitioner. This is not specifically tied to free movement of people but applies to any implementation of effective border control.

The authors are thankful for the inputs received and have taken great care to ensure that this document accurately reflects the conversations that were held. Any errors or omissions are the author's own.

2. How to use this guide

This is not the kind of guide you pick up and read from beginning to end as if it were a novel. It is a reference book, the kind you pick up, turn to a random section and start reading. This guide is not intended as an assessment of existing initiatives for free movement of people, though it does pick up learning points from current initiatives in this area. Nor is it a “cook-book”, model or prescription how to implement one. This guide is intended to provide an introduction on the subject to all involved, and to raise awareness and knowledge for all stakeholders.

STRUCTURE OF THE GUIDE

Inside this guide, the principal topics are arranged in four parts. Each part breaks down into chapters that cover various aspects of the parts main subject. Within these chapters you will find sections formulated as questions that might be relevant to you.

“Part I: Getting started” is an introduction to the subject of free movement of people;

“Part II: Building consensus on intergovernmental level” is the first element of implementation, covering the policy aspects. Essentially, it handles Theme A.

The following two parts are rather technical and operational:

“Part III: Designing the credentials” addresses Theme B;

“Part IV: Designing an appropriate Border Management” covers Theme C.

Finally, the first annex is a rather deep introduction on some technological fundamentals, you might find helpful to read into, when your curiosity goes beyond what is written in parts 3 and 4:

annex 1: “Some technological fundamentals”

It has 13 chapters (plus four in annex), each one covering a specific aspect of managing Free Movement Zones - such as developing the international dialogue, setting up the credentials and managing the borders. Just turn to the chapter you’re interested in and start reading.

3. Icons used in this guide

MORE READING AND ADDITIONAL RESOURCES

Here you will get additional links and resources for additional reading.



SUMMARY

Here you will find an abstracted information from another part or chapter for better context.



TAKE CARE

Important learnings or frequent misconceptions are highlighted here, to make sure you are fully aware.



REFERENCE / SAMPLE

Taking a look at experience or good-practices from other implementations.



CHECKLIST

A list of sample points recommended for consideration.



4. Interaction and future work

This guide is made for you: it is here to answer practical questions for policy makers and people engaged in various aspects of operations. Therefore, we love to hear back from you on further questions and wishes. This will help us to develop an updated edition in the future. Also, this guide contains information subject to ongoing development. Should you want to point out to something needing an update, you may kindly reach out, too.

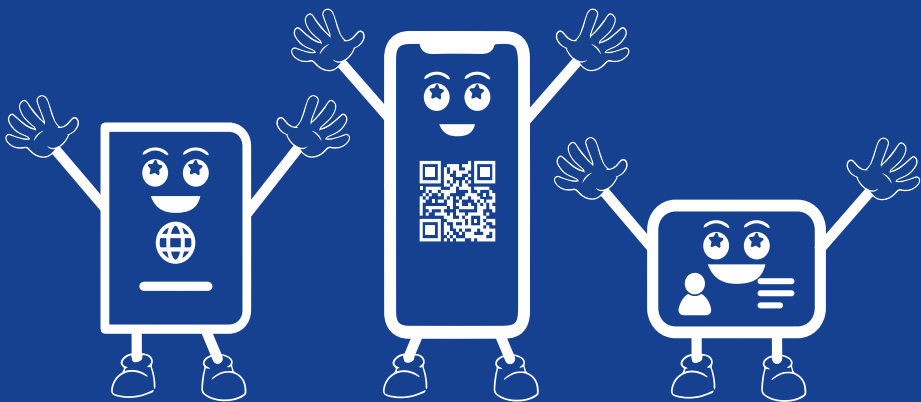
On our agenda for a next edition are the topics “information exchange” and “procurement”.

Please send your specific question or remark to idguide@iom.int for our review. You will receive an automatic reply confirming receipt. We will review each email. However, please understand that we will not answer personally to each and every received eMail.

PART I

GETTING STARTED

Let's get started!





INTRODUCTION TO THIS PART

First of all, we will need to be clear on what we will be talking about. So, chapter 1 will introduce the various protocols that are established for allowing free movement of people. This will be about the different terminology and types, and also the reasons to actually contemplate the implementation of such a protocol. We then define a new term, Free Movement Zone (FMZ) to cover the various existing initiatives and harmonising the various terms that are currently used to describe free movement of people. We also define the characteristics of such a zone. We point out the things to consider before you embark on this interesting undertaking of establishing a Free Movement Zone. And finally, a high-level overview of examples of implementations of FMZ.

CHAPTER 1

WHAT ARE FREE MOVEMENT ZONES



What you will learn about in this chapter:

- The background for establishment of Free Movement Zones
- A sample of the different types of travel arrangements that can be found around the globe
- Differences between the various models
- Definition of a Free Movement Zone and characteristics of such a zone

5. What is meant by 'Free Movement'

“Would you tell me, please, which way I ought to go from here?”
“That depends a good deal on where you want to get to.”
“I don't much care where –”
“Then it doesn't matter which way you go.”

Lewis Carroll, *Alice in Wonderland*.

Freedom of movement, mobility rights or the right to travel is a human rights concept that encompasses the right of individuals to travel from place to place within the territory of a country, as well as the right to leave and return to that country. This includes not only visiting places, but also changing the place of residence or work.

Freedom of movement within a country encompasses both the right to travel freely within the territory of the State and the right to relocate oneself and to choose one's place of residence.

Jérémiée Gilbert, *Nomadic Peoples and Human Rights* (2014), p. 73

It is important to note that UN Member States have a sovereign right to determine immigration into their country. It is their right to determine the rules that will be applied to assess the admissibility of a non-citizen and also allow them to have differentiated rules for specific groups of travelers. They also have the right to decide on the eligibility of the traveler to stay and take up residence in their country.

Most protocols that allow free movement of people are based on some core principles. They usually form part of a Regional Trade Agreement (RTA).

Many WTO members are involved in negotiations to create new RTAs. Like existing agreements, most new negotiations are bilateral. However, a more recent development is negotiations

and new agreements between several WTO members. These include developments in¹ :

- the Asia-Pacific region - for a Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) Agreement, between 11 parties;
- Within Asia - between members of the Association of Southeast Asian Nations (ASEAN) and other six WTO members with which ASEAN has agreements in force (the Regional Comprehensive Partnership Agreement);
- In Latin America - with the Pacific Alliance between Chile, Colombia, Mexico and Peru; and
- In Africa - with the tripartite agreement between the parties to the Common Market for Eastern and Southern Africa (COMESA), the East African Community (EAC) and the Southern African Development Community (SADC), and the African Continental Free Trade Agreement (AfCFTA).

Such multilateral agreements need to consider free travel as an integral part of these agreements for them to be successful.

“ Freedom of movement did not only amount to the right to travel freely, to take up residence and to work, but also involved the enjoyment of a legal status characterised by security of residence, the right to family reunification and the right to be treated equally with nationals. ”

Kees Groenendijk, Elspeth Guild, and Sergio Carrera, *Illiberal Liberal States: Immigration, Citizenship and Integration in the EU (2013)*, p. 206

There exist different arrangements to allow such movement of people across borders.

¹ From: https://www.wto.org/english/tratop_e/region_e/region_e.htm

6. What are the different types of existing travel arrangements

There are many variations of free travel arrangements, starting with the managed right of travel, to full removal of borders with right to settle in another country's territory. In this guide, we will take a look at some of the options for implementation and reflect on their characteristics.

Some of the travel arrangements include the removal of borders between countries. The absence of borders is not the same as abolishment of border policing activities. Within the Schengen area there is a complete removal of regular border control/fences. In the sense of law enforcement there are border police activities within the territories, which means that identity documents still play a part, even in the absence of borders.

The development of the Schengen Free Movement Zone is a direct consequence of allowing for free movement of people, whether they be citizens or not. This is only possible by establishing a common external border, a common visa and an entry/exit system, all of which were latter day developments. The EU initially focused on the movement of citizens and residents only. However, with borderless travel possible, it became necessary to handle other travellers (those who were not citizens or residents) and the Entry/Exit System is still a work in progress.

In some global regions there is *de facto* free travel, although not intentionally. It occurs as a consequence of lack of terrestrial border controls. While this is recognised as a security threat, action is rarely taken to remedy the situation.

Even when free movement of people does exist, it is likely that border control and immigration checks will still be applicable for border crossings. The only difference would be differentiated treatment based on the nationality or citizenship of the traveller. This may be in the form of separate lanes for immigration, visa free entry, automatic permission to stay for a certain number of days etc.

To disentangle the various schemes that exist and to harmonize the concept of what a free movement arrangement should look like, it is necessary to get a quick overview of existing travel arrangements. A few of them are listed below.

Encyclopedia Britannica defines a 'free-trade zone', also called a 'foreign-trade zone', formerly 'free port', as an area within which goods may be landed, handled, manufactured or reconfigured, and re-exported without the intervention of the customs authorities. Only when the goods are moved to consumers within the country in which the zone is located do they become subject to the prevailing customs duties. Free-trade zones are organized around major seaports, international airports, and national frontiers—areas with many geographic advantages for trade. Examples include Hong Kong, Singapore, Colón (Panama), Copenhagen, Stockholm, Gdańsk (Poland), Los Angeles, Shannon (Ireland), and New York City.

FREE-TRADE
ZONE OR
FOREIGN-TRADE
ZONE

ALSO:
ECONOMIC FREE
TRAVEL ZONES
/ COMMON
TRAVEL AREAS

The primary purpose of a free-trade zone is to remove from a seaport, airport, or border those hindrances to trade caused by high tariffs and complex customs regulations. Among the advantages of the system are the quicker turnaround of ships and planes through the reduction in formalities of customs examinations and also the ability to fabricate, refinish, and store goods freely.

Free travel can be found in combination with foreign-trade zones. Then, terms such as 'Economic Free Travel Zone' or 'Common Travel Areas' can be found.

Registered Traveller (also known as 'Trusted Traveller') programmes may allow a specific category of travellers (e.g., business travellers, or from a world region) to avoid more rigorous screening at the border, the requirement to make customs declarations and/or complete disembarkation cards. As such, 'Trusted Traveller Programmes' are established to allow concessions on travel and entry/exit formalities. This status is granted upon application of such traveller and favourable assessment against the qualification criteria. While a Trusted Traveller scheme is not the same as 'free movement

TRUSTED
TRAVELLER
SCHEMES /
REGISTERED
PROGRAMMES

of people', it could be an implementation mechanism for such an arrangement.

Often Automatic Border Control systems (ABC) are used to process this set of travellers who are assessed as low risk. Participants in such programmes will be enrolled and vetted by border control agencies before being allowed to use the system. Nevertheless, 'watchlist' checks will still be carried out, and travellers can be required to submit to comprehensive screening.

BORDER FREE AREAS

Based on agreements, the internal borders of Border Free Areas are subject to minimal controls, if any, and can normally be crossed by the nationals of the territory with minimal identity documents (with certain exceptions). Such exceptions could be persons with legal prosecutions ongoing or rulings, preventing them from leaving the territory. The maintenance of Border Free Areas involves co-operation on immigration matters between authorities. A consequence of such arrangements is the handling of border crossing by people who are not citizens or residents of the Member States in question.

Examples of these are the European Schengen Area, and the Common Travel Area between the United Kingdom, the Republic of Ireland, the Isle of Man and the Channel Islands.

PASSPORT-LESS BORDER CROSSING

Crossing international borders usually requires travellers to carry and present their passport. For countries with specific treaties, this requirement can be dropped, and replaced by other defined, acceptable means of identification such as ID-cards.

Prior to the Schengen agreement, such arrangements existed between Switzerland and their neighbouring countries Germany, France, Italy, Austria, where the national ID card was sufficient to cross the borders, even with a tolerance of 6 months past its expiry. Since then, this agreement has been replaced and broadened.

Travel Bubbles are not actual Free Movement Zones. They are rather pragmatic and ad hoc agreements responding to a sudden situation, such as a pandemic, a security or migration crisis. IATA defines a Travel Bubble as “a State-level agreement that enables international air travel between two (or more) countries based on a mutually agreed set of public health mitigation measures. In some markets, reference is made to ‘travel corridors’ or ‘airbridges’.² The definition of the travel bubble can be expanded beyond international air travel and comprise any means for border crossing.

The purpose of ‘Travel Bubble’ arrangements is to facilitate the reopening of bilateral travel markets on common travel criteria.

This term has become popular in the context of international crisis, such as during the Covid pandemic.

Its advantage is the rather quick implementation in times of need, as well as modifications or termination. However, a Travel Bubble is not the same as a Free Movement Zone. It simply means that a pre-condition for travel (for example, negative Covid tests or full vaccination status) is waived between members of a travel bubble.

We mention travel bubbles to illustrate the point that free travel arrangements should be able to respond to changing security, public health and migration challenges – of which Covid is merely the current example.

7. Definition of FMZ for the sake of this guide

Despite various implementations of Free Travel Zones or Free Movement Zones, there are barely any recognized definitions and terms.

² Websource: <https://www.iata.org/contentassets/5c8786230ff34e2da406c72a52030e95/restarting-international-aviation-through-travel-bubbles.pdf>, accessed on May 20, 2021

For the sake of this guide, we define a Free Movement Zone (FMZ) as an agreement between member countries that establishes a community which supports the free movement of goods, services and people across international boundaries with special privileges for citizens/residents (or a defined subset of this group) of the member countries.

The characteristics of such a FMZ are generally as follows:

- It could be a bilateral arrangement between two countries, but is usually a multilateral agreement between countries that are part of a contiguous geographical area.
- Defined for specific groups of citizens/residents of the member countries and specifies differentiated rules of entry/exit and stay.
- May lead to open borders between the member countries.
- In case border controls still apply, the freedom to travel using identity documents that are not necessarily passports.
- Involves a high level of mutual trust between the members of the community.
- They are usually complimentary in size and composition of populations and labour markets.
- Have similar levels of institutional maturity, specifically in terms of their legal systems.

CHAPTER 2

WHAT ARE THE REASONS TO ESTABLISH FMZs? AND WHY NOT?



In this chapter we will ask ourselves several questions, both in reflecting the usefulness of a FMZ and how to define boundaries for an FMZ.

- What are the advantages and disadvantages of free movement of people or work force?
- Who benefits and loses from this free movement?

There are many considerations for establishing a FMZ. These could be political, economic, social or security considerations. Below, we highlight some points to reflect on, in four sections:

- [section 8: “Political considerations”](#)
- [section 9: “Economic considerations”](#)
- [section 10: “Social considerations”](#)
- [section 11: “Security considerations”](#)

8. Political considerations

The establishment of an FMZ requires co-operation between multiple political players. If these are not considered, this may hinder or block the establishment of an FMZ. The various advantages/disadvantages requiring political considerations include:

PRO



- Strengthening bi-/multilateral cooperation among states, which can be both goal and consequence of establishing the FMZ.
- Free movement of economically active workers can be turned into the free movement of people. In other words, you don't need to move to a member country to work; you could also go there to 'retire in the sun'. This expands the economic rule-sets into a more politically integrated vision for the FMZ (e.g., Maastricht Treaty 1992 for the EU).
- Can serve to avoid conflict and promote harmony between the FMZ nations. Free movement of people across national borders can possibly diminish national rivalries because countries tend to become more integrated.
- Free movement of labour should help reduce regional disparities between the economic union. In the EU, for example, free movement of labour has enabled workers in the former Eastern bloc countries to avail of work opportunities and increase living standards. Some of this income will be saved and sent home to increase living standards in Eastern Europe. After joining the EU, countries like Portugal, Spain and Ireland moved closer to average EU GDP per capita levels.

CON

- Social tensions caused by migrants that are not fully recognized or accepted by the authorities and/or the public.
- Migration of unskilled workers, which may not be welcome and which may lead to competition within the work force with resulting pressure on the political landscape.

9. Economic considerations

The effective utilization and allocation of the economic resources of the members of the FMZ is both a driver and a concern when establishing an FMZ. Advantages and disadvantages include:

PRO

- Facilitating trade and cross-border investment.
- Economic growth and removal of significant imbalances between countries in terms of their national development.
- Removal of red tape and protectionism through common customs procedures and common external tariffs.
- Common trade deals with foreign partners.
- Allows for greater bargaining power when negotiating trade deals.
- Economies of scale related to investments in identity and border management systems and components.
- Increase in overall demand through higher consumption by the mobile workforce.
- Flexible labour markets with possibility to recruit from a larger talent pool. Permit not needed to work in another country.
- FMZs can help manage demographic challenges posed by a rapidly ageing population, which places strain on public finances because people over the age of retirement turn into net recipients of state spending (pensions and healthcare, less income tax contributions). Free movement of labour can see young immigrants come to areas of declining working population and make a net contribution to public finances.

CON

- Competition from the work force in neighbouring countries can push down wages or lead to higher unemployment rates. This may be mitigated by a growing population creating higher demand for goods and services. The section of the work force possibly under pressure are unskilled workers, at risk of displacement from immigrant labour.
- Highly skilled workers may be attracted to higher developed countries with higher wages, making it difficult for developing countries to retain skilled staff. This could harm economic development in developing countries.
- Risk of large migrant flows from low-income to higher income countries. This can cause economic and social problems. In theory, an increase in the working population should directly increase GDP, leading to greater tax revenues that can be used to spend on improving public services. However, this will only happen if the economy can make use of the work force, otherwise there can be pressure on infrastructure capacity and social-welfare schemes.
- During a phase of economic growth, immigrants, workers and their families may be welcome (or at least tolerated) in support of growth. However, on the downswing, it often isn't that easy to return this population to their country of origins. It actually might be against the spirit of the free travel agreements set in place.
- For countries with traditional visas and immigration fees in place, there could be a considerable or potential loss of visa revenue. This might not be of great concern in the big picture. However, it could be reason for pushback from the concerned stakeholders.

10. Social considerations

The interests and aspirations of the community and society is possibly the greatest factor that will help in the success or failure of a Free Movement Zone and must be considered in its establishment.

PRO

- Working migrants from within the FMZ can be more easily processed and handled when the relevant arrangements are defined within the FMZ.
- Free movement of labour gives increased opportunities to workers and makes labour markets more flexible. Their options grow for 'grass-root' welfare.
- Socially/historically-related groups on both sides of the borders are no longer divided and can cross borders legally.
- If so defined by the treaty, educational and professional qualifications can be universally accepted across the FMZ, and in theory, there should be no discrimination for firms choosing between native and migrant workers.

CON

- Poorly defined and operated FMZ-agreements can cause social distress and unrest. This can be a consequence of more working migrants and dropping wages, pressure on public infrastructure, a clash of cultures, etc., just to mention a few possible triggers.
- A net growth of population by migration can precipitate for a housing and infrastructure crisis (such as schools, medical treatment, transportation capacity etc).
- Even if provision of public services and housing can increase to meet demand, a rising population can lead to a decline in quality of life because it increases population density and congestion.

11. Security considerations

The establishment of a Free Movement Zone reduces possible conflicts between the members. This was a key driver for the establishment of the EU and was seen as a mechanism to prevent future wars. This is also the key driver for some of the developments on the African continent. A Free Movement Zone allows members to address security in a coordinated manner and helps lessen the burden of individual states to maintain security.

PRO

- Potential grounds for a common peacekeeping force.
- Strengthened, commonly directed exchange platforms for security strategy and response.
- Lends impetus to standardization of cross-border identity document systems and improves quality and interoperability of such systems.
- Cross-border law enforcement could be improved, if considered a topic that is regulated in the FMZ-treaty.

CON

- Social unrest and instabilities, if major uncontrolled migration happens. Criminal groups can expand their field of operation, especially when internationally coordinated law enforcement is not facilitated.
- Possible social insecurity and commercial impact upon the migration of criminality.

12. Who benefits and loses from this free movement

In the previous section, we detailed the pros and cons of allowing free movement of people and labour.

Some stakeholders impacted by the benefits and losses from free movement include employers seeking workers, entire industries providing services and infrastructure for the additional population living or travelling in the country, the tourism sector, families and individuals. See [section 26: “For which user groups”](#) for a more detailed view of such groups. Below, we will consider the country level perspective:

Countries from which labour migrates get the following advantages:

- Relieves pressures on unemployment.
- Remittances sent by migrant workers abroad adds to the economy.
- Allows knowledge transfer when these people return to their country of origin.

There might be disadvantages as well:

- Reduction in the potential workforce.
- 'Brain drain'.
- Deflation due to reduced economic activity.

Countries, which receive migration could enjoy these potential advantages:

- Reduced labour shortage.
- 'Brain gain'.
- Increase in economic activity.

On the flip side, they may also face some disadvantages:

- Reduction in employment opportunities for low skilled workers.
- Cultural differences leading to stress fissures.
- Increased demand on infrastructure like housing, healthcare and education.
- Inflation.

It is important that these effects are well understood before embarking on the establishment of a Free Movement Zone. It will be successful if, and only if, all the participants in such a scheme see a net benefit in engaging in such an arrangement.

A good resource to consider on the benefits of free movement to the work force is the International Labour Organization (ILO):

https://www.ilo.org/employment/areas/WCMS_DOC_EMP_ARE_TRE_EN/lang--en/index.htm



CHAPTER 3

WHAT DO YOU NEED TO CONSIDER WHEN ESTABLISHING FMZs?



You have looked at the characteristics of FMZs and consider the advantages to exceed the disadvantages. Now you would like to understand how to proceed more specifically and check, if you are set up for this journey.

- What are the prerequisites for successfully implementing an FMZ?

13. Are there pre-requisites for establishing an FMZ

When embarking on the journey of establishing a free travel protocol or FMZ, it is important that all stakeholders be identified and prepared for what lies ahead. We will want to highlight some of the challenges you should prepare for when setting up and eventually operating and maintaining this area of closer multi-national cooperation are discussed below.

HUMAN CHALLENGE

The first thing to understand about developing and rolling out an FMZ is the complexity of deploying a harmonised initiative across multiple human stakeholders. While the ultimate outcome of the initiative is to implement policy and technology for cross-border travel and migration by air, land and sea borders, in reality, this is an overwhelming challenge to the stakeholders and the personnel involved.

From negotiating major budgets with government officials to training of officers, successful deployment revolves around coordinating stakeholders at all levels to work towards a shared vision of success.

Having a good relationship and a high level of trust among the states at all levels is a corner stone in developing a successful scheme and operation.

ALIGNING ON OBJECTIVES AND RESOLVING CONFLICTING INTERESTS

When considering the implementation of a Free Movement Zone, it is crucial to align on the objectives of each member state. There is no standard solution and it is in the hands and negotiation skills of all members to develop a mutually beneficial variant. It is advisable to apply a methodology starting at the level of problem to be improved, and avoid jumping to conclusions.

A methodology that might be worth considering is the Investment Logic Mapping³.

At its heart are the questions: What is the problem you are trying to solve and to what extent will the investment solve it.

³ The Investment Logic Map is the first artifact created under the Investment Management Standard (IMS) defined by the Australian State Government of Victoria - Department of Treasury and Finance. Aspects of the IMS had been evolving since 2004 within the state government, and they were formalized into the Investment Management Standard in 2007.

In this case, the investment is the mutual policy or system. In the course of this process, you will move from the Problem to the Benefit to the Strategic Response to Solution Options.

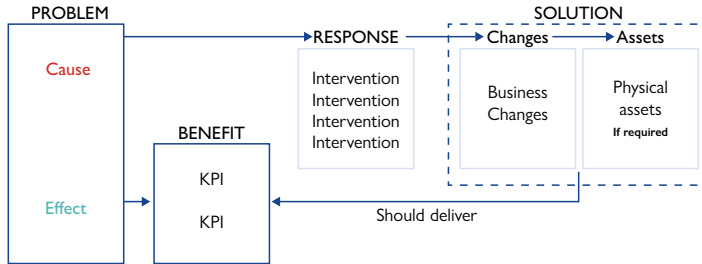


Figure 1 – Chart explaining the principle of an Investment Logic Map⁴

It's important to consider the social, economic and political challenges of deploying a standardized policy and perhaps technical solution across multiple nations. There will likely be challenging discrepancies that result in diverging attitudes towards a Free Movement Zone. These discrepancies can originate in historic rivalry, in diverging interests or struggles for dominance.

AVOIDING CROSS-BORDER FRICTIONS

Such free travel initiatives can require aligning policing and border-management tools. While the development and implementation of such systems across the Member States can pose a challenge in itself, the capability to handle existing systems is important. Establishing a clear view of the current systems architecture is key to understanding the practical requirements for each member state to reach compliance with the harmonized or interoperating systems. Providing sufficient funds and capable resources is a first step in the right direction.

“ I have not failed. I've just found 10,000 ways that won't work. ”

– Thomas A. Edison

MANAGING FAILURE

⁴ Document: Investment Management Standard 2017 Departmental User Guide. By the Victoria State Government Department of Treasury and Finance. 2017. <https://www.dtf.vic.gov.au/infrastructure-investment/investment-management-standard>

As with any pan-national initiative, there will naturally be some difficulties and challenges. For example, in the EU's free travel scheme, ever since the EU Commission's suggestion of its Smart Borders package in 2008, stakeholders at all levels have faced unusual set-backs, unforeseen obstacles, and uncontrollable errors. (See chapter 5: "Getting started", section 24: "Establishing political will and operational engagement" for some of the experiences.)

It is important to accept the inevitability of some setbacks with an undertaking of this scale. While most people view failure as a negative outcome or an inability to reach a given goal, developing resilience against failure and understanding how to move forward is critical to get closer to success.

Fostering an organisational culture that views failure as an exercise that provides learning points to inform future decisions is important. The sheer volume of unknowns and uncontrollable variables in an undertaking of this magnitude requires highly skilled and resilient political, policy, technical and operational teams that can adhere to rigorous standards regardless of the circumstances. It is the 'exceptions' that often break a new system. Accepting that from the outset, and knowing that you cannot identify most exceptions until they occur, is vitally important.

If the stakeholders involved take a rigid and administrative approach that leaves no room for agile adaptations to new insights, a single mistake can throw the entire operation into disarray.

Introducing new processes requires substantial training for on-the-ground personnel and a steep learning curve that will inevitably result in mistakes. Therefore, make sure you are capable of establishing a solid training and support force, to achieve the objectives of processing and security. Opening up experience exchange channels between the countries already prior to setting up an FMZ will be most beneficial to the project and all stakeholders.

Also, incremental steps instead of a 'big bang' approach, will support your organizations. In the IT-world we probably would call it 'Agile methodology'. The development of the Schengen Zone in small increments is a very good example of how small steps can lead to an FMZ. Again: see above referenced section in chapter 5: "Getting started".

SOFT LAUNCHES AND INCREMENTAL STEPS

CHAPTER 4

EXAMPLES OF FMZ INITIATIVES



There are many FMZ initiatives in progress. All of them can best be described as a work in progress. All of them have rules or principles, or in some cases, laws that provide for the free movement of people, along with goods and services, but in practice, the free movement of people is not implemented in many of the cases. We do not intend this chapter to be an exhaustive review or analysis of the different examples, but simply record them to show that such initiatives already exist. This will help to understand that FMZs come in different shapes and sizes.

14. European Union



Free movement of people, goods and services are guaranteed under the charter. People are free to travel, shop and work anywhere within the bloc, without regular border controls. The original intent was to integrate the economies to avoid any possible future conflicts between European countries.

Characteristics

- Economic growth and removal of significant imbalances between countries in terms of their national development.
- Flexible labour markets with possibility to recruit from a larger talent pool. Permit not needed to work in another country.
- Increase in overall demand through higher consumption by the mobile workforce.
- Larger market for European goods without tariffs and trade barriers.
- Greater bargaining power when negotiating trade deals with foreign partners.

A historic abstract of the development steps is provided in [section 24: “Establishing political will and operational engagement”](#) as a sample, illustrating the process and some learnings. While the EU is well advanced in its implementation as a Free Movement Zone, there do exist some challenges. For example, a Schengen wide entry/exit system is not in place, though it is being discussed and planned at this moment. It is expected to be operational in the first half of 2022. Furthermore, the crises precipitated by the migration of refugees, which resulted in the imposition of border control between Member States, often in an uncoordinated manner, underlines the need to have such contingency planning as part of the design process of FMZs.

15. Common Travel Area (UK, Ireland)



The Common Travel Area (CTA) is an open-border area comprising the United Kingdom, Ireland, the Isle of Man, and the Channel Islands. The British Overseas Territories are not included. Based on agreements that are not legally binding, the CTA's internal borders are subject to minimal, if any, controls and can generally be crossed by British and Irish citizens with minimal identification, with some exceptions (e.g., Such citizens must show identification to board a ferry or an airplane, and some airlines and sea carriers only accept a passport as valid identification). Maintaining the CTA involves cooperation on immigration issues between the British and Irish authorities.

In 2014, the British and Irish governments began a trial system of mutual recognition of visas for onward travel within the CTA. As of June 2016, it applies to Chinese and Indian nationals and is limited to certain visa types. Other nationalities and individuals on non-qualifying visas continue to require separate visas to visit both countries and cannot claim a transit visa exemption if they wish to travel through the UK to Ireland.

Since 1997, the Irish government has introduced systematic identity checks for air passengers arriving from the United Kingdom and selective checks for sea passengers, as well as occasional checks on land entries.

With the exit of the UK from the EU at the end of 2020, the Irish – UK border on the island of Ireland became an external border of the European Union. The UK Immigration Act 1971 was amended by adding “An Irish citizen does not require leave to enter or remain in the United Kingdom”. The Act repeals free movement rights for other EU citizens from 1 January 2021, but makes exceptions for Irish citizens. Guidance from the government also states: “Irish citizens will continue to be able to enter and live in the UK as they do now.”

A unique fact: UK and Irish citizen can vote in each other's parliamentary elections if resident on the other's territory.

16. Oceania



We see four major groupings suggesting a kind of limited free-travel zone. The citizens of these countries can travel on a common document from the affiliated country; however, their nationality is marked in the passports. Cross-border activities are mostly related to work, health services and studies. These topics would be worth supporting the establishment of a Free Movement Zone. However, it is to be considered that there are very few direct connections among the members. Much travel by air takes place via Hong Kong or Japan. Therefore, air-travel passengers are still required to hold passports for this kind of trip.

Countries sharing passports with New Zealand:

- Cook Islands;
- Tokelau;
- Niue.

Countries affiliated with the USA:

- American Samoa;
- Guam;
- Northern Mariana Islands;
- United States Virgin Islands;
- Selection of Minor Outlying Islands.

Former French territories:

- Clipperton Island;
- French Polynesia, with the Island Tuamotu Archipelago;
- Marquesas Islands;
- Gambier Islands;
- New Caledonia;
- Wallis and Futuna.

Australia / New Zealand

The free travel zone between Australia and New Zealand, and the associated Closer Economic Relations Trade Agreement (ANZCERTA) is notable. Its architecture is very large both in travel volume, capital movements and trade in goods and services than most of the other examples.

The mutual recognition of goods and occupations removes technical barriers to trade and impediments to the movement of skilled personnel between jurisdictions without the need for complete harmonisation of standards and professional qualifications.

17. Caribbean Community (CARICOM)

CARICOM is the oldest surviving integration movement in the developing world. It is a grouping of twenty countries: fifteen Member States and five Associate Members. It targets a single market for goods and services, and in part allows for free movement of people with some limitations.



CARICOM describes its member countries as sharing similarities and challenges. On the one hand they are all in proximity to major markets in North and South America, and most countries, have had to make the transition from agriculture or mining to a service-driven economy (especially in tourism and financial services). On the other hand, they have to overcome the challenges of frequent natural disasters, in addition to small size (with associated lack of economies of scale and vulnerability to external shocks).

The Member States are:

Antigua and Barbuda*, Bahamas, Barbados, Belize, Dominica*, Grenada*, Guyana, Haiti, Jamaica, Montserrat*, Saint Lucia*, St Kitts and Nevis*, St Vincent and the Grenadines*, Suriname, Trinidad and Tobago.

The Associate Members are:

Anguilla*, Bermuda, British Virgin Islands*, Cayman Islands, Turks and Caicos Islands.

Characteristics:

- Economic growth and free flow of investments;
- People are free to travel, but need to apply for permission to work and live in another country;
- Common trade deals with external parties.

There are multiple sub groupings within CARICOM with varying approaches. For example, the Organization of Eastern Caribbean States (OECS; Countries marked above with Asterix *; Additionally, Martinique and Guadeloupe) has a quite extensive level of integration.



IOM published a research paper on Free Movement in the Caribbean in 2019, that provides an extensive research data base on the subject.

https://publications.iom.int/system/files/pdf/free_movement_in_the_caribbean.pdf

18. Southern Common Market (Mercosur/sul)



Mercosur (in Spanish), Mercosul (in Portuguese) officially translates to English as Southern Common Market, and is a South American trade bloc established by the Treaty of Asunción in 1991 and the Protocol of Ouro Preto in 1994. Its full members are Argentina, Brazil, Paraguay and Uruguay. Venezuela is also a full member but has been suspended since 1 December 2016. Associated countries are Bolivia, Chile, Colombia, Ecuador, Guyana, Peru and Suriname.

The purpose of Mercosur is to promote free trade and the free flow of goods, persons and currency. Since its inception, Mercosur's functions have been updated and modified several times; it is currently limited to a customs union in which there is free intra-zone trade and a common trade policy between member countries. It has a common external tariff for imports. Free movement of people was envisaged in the original declaration, but now confines itself to a customs union.

Characteristics:

- Economic growth and free flow of investments across national boundaries;
- Flexible labour market with some limitations. People still need to apply for a permit to be allowed to work in a different country;
- Common external tariff protects local industries.

19. Common Market for Eastern and Southern Africa (COMESA)

A free trade area that is mainly focused on free movement of capital and goods, with common external tariffs.



Member Countries are:

Burundi, Comoros, DR Congo, Djibouti, Egypt, Eritrea, eSwatini, Ethiopia, Kenya, Libya, Madagascar, Malawi, Mauritius, Rwanda, Seychelles, Sudan, Uganda, Zambia, and Zimbabwe.

Characteristics:

- 9 of the members have a free trade agreement with elimination of tariffs for goods originating in one of the nine Member States;
- Greater harmonization achieved in financial services;
- Free movement of people – still restricted.

20. East African Community (EAC)

Common market for goods, labour and capital, and eventually a political federation.



Member Countries are:

Burundi, Kenya, Rwanda, South Sudan, the United Republic of Tanzania, and Uganda.

Characteristics:

- Common external tariff on imports;
- Free trade area and common customs procedures;
- Free movement of people still restricted.

21. Economic Community of West African States (ECOWAS)

ECOWAS is a regional political and economic union, consisting of 15 countries in West Africa aimed at economic integration within the members.



Consists of two sub blocks. West African Economic and Monetary union (WAEMU), which share a customs union

and a common currency and West African Monetary zone (WAMZ) which also expects to have a common currency.

ECOWAS is meant to foster interstate economic and political cooperation. It was established through the Treaty of Lagos (1975). This treaty underwent a revision in 1993, which expanded the scope and powers of the treaty.

The Member States are:

Cape Verde, Gambia, Guinea, Guinea-Bissau, Liberia, Mali, Senegal, Sierra Leone, Benin, Burkina Faso, Ghana, Ivory Coast, Niger, Nigeria and Togo.

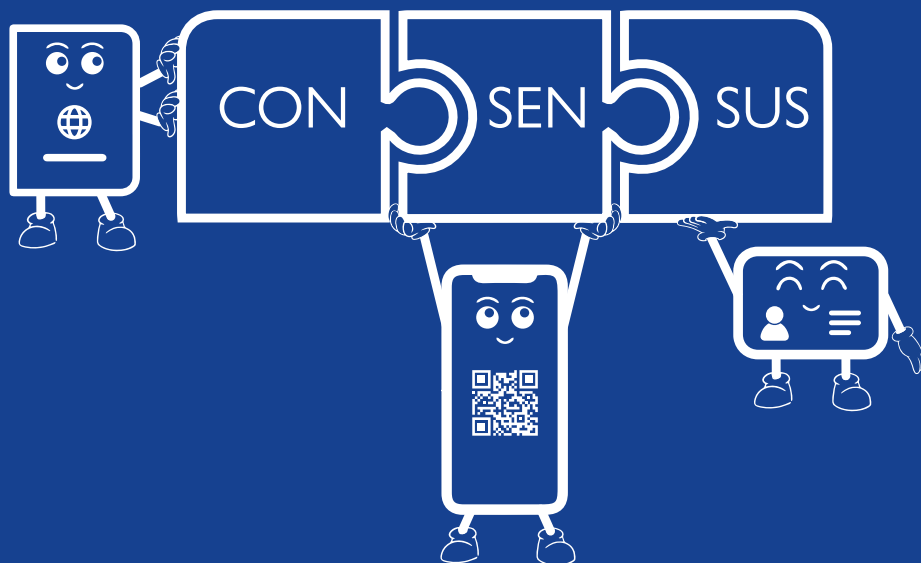
Characteristics:

- Common External Tariff (CET);
- Stated objective of a borderless region which is integral in the facilitation of regional integration and establishment of a common market;
- Enshrines the 'Right of residence', which is the right granted to a citizen who is a national of one Member State to reside in a Member State other than his State of origin;
- Establishment of a National Identity card (with a common design and specification across ECOWAS) as a travel document within the ECOWAS Region⁵.

⁵ <http://www.ecowas.int/wp-content/uploads/2015/01/3-Travel-Certificate.pdf>

PART II

BUILDING CONSENSUS ON INTERGOVERNMENTAL LEVEL





INTRODUCTION TO THIS PART

This part covers Theme A that we mentioned in the beginning of this guide. It is intended as a conspectus of the drivers and considerations of the establishment of an FMZ.

In this part, we discuss the starting point of this venture, with defining objectives, getting buy-in from stakeholders, and how harmonization and standardization can help on this way. We also review a number of topics that need to be discussed and decided, as a foundation for the implementation work.

CHAPTER 5

GETTING STARTED



What you will learn about in this chapter:

- Defining your desired outcomes from the establishment of a Free Movement Zone, and finding common grounds with your international partners
- Making sure the political will is strong enough for the whole process
- How harmonization and standardization can help you along the way

22. What are our priorities

Free Movement Zones bring opportunities and can improve the situation for your economy and citizens, while growing the relationship with your neighboring countries.

In chapter 2: “What are the reasons to establish FMZs? And why not?” we discussed advantages and disadvantages of free travel protocols. Obviously, you will be looking for more of the first, and less of the latter.

Below checklist can serve as inspiration, and as preparation for talks.

CHECKLIST



Where lie your priority interests?	
Political	
<input type="checkbox"/>	a) Strengthening bi-/multilateral cooperation; b) Forming stronger political negotiation powers towards other blocs or major countries, including creating synergies in governance?
<input type="checkbox"/>	a) Facilitating free movement of people even for non-economic reasons, and b) Realizing a politically more integrated vision?
<input type="checkbox"/>	a) Promotion of harmony, reduction of conflict and diminishing rivalries; b) Becoming more integrated?
<input type="checkbox"/>	Reduction of regional disparities between the member countries?
<input type="checkbox"/>	...
<input type="checkbox"/>	...
Economy	
<input type="checkbox"/>	Facilitation of trade and cross-border investments?
<input type="checkbox"/>	a) Drive economic growth; b) Remove significant imbalances between countries in terms of their national development?
<input type="checkbox"/>	a) Establish common customs procedures and common external tariffs; b) Protect local industries?
<input type="checkbox"/>	Facilitate common trade deals with foreign partners?

<input type="checkbox"/>	Greater bargaining power when negotiating trade deals?
<input type="checkbox"/>	Drive overall demand through higher consumption by the mobile workforce and people choosing to change their place of living?
<input type="checkbox"/>	Make labour markets more flexible, with possibility to recruit from a larger talent pool?
<input type="checkbox"/>	Manage the demographic challenges, posed by a rapidly ageing population?
<input type="checkbox"/>	...
<input type="checkbox"/>	...
Society	
<input type="checkbox"/>	Establish easier processes for handling working migrants?
<input type="checkbox"/>	a) Increase opportunities to workers; b) render labour markets more flexible?
<input type="checkbox"/>	Clarify the situation of socially/historically related groups on both sides of the borders on their cross-border movements?
<input type="checkbox"/>	a) Reduce discrimination of work force; b) Harmonize work qualifications?
<input type="checkbox"/>	...
<input type="checkbox"/>	...
Security	
<input type="checkbox"/>	Support common peacekeeping force efforts?
<input type="checkbox"/>	Strengthen exchange platforms for security strategy and response?
<input type="checkbox"/>	Formalize and implement global standardization efforts of cross-border identity document and border management systems?
<input type="checkbox"/>	Improve law enforcement efforts even beyond the borders in a cooperative manner?
<input type="checkbox"/>	Improve management of and response to migration from outside the potential FMZ-Member States?
<input type="checkbox"/>	...
<input type="checkbox"/>	...

Table 1 – Checklist with Priority of interests

23. How do you find a minimal common interest and anticipate blocking points



“Spirits that I've cited – my commands ignore”

- Johann W. v Goethe, *The Sorcerer's Apprentice*

This famous rhyme can be a word of cautioning on the subject of defining scope, establishing common interests and handling blocking points. Be aware, that opening these discussions with your potential FMZ-partners will touch sensitive points of national interests. These discussions have the potential to escalate, if not well mastered, and you can lose control.

In the above table 1: “Checklist with Priority of interests” most objectives have the potential of a win-win situation for all signing countries. However, that is the ideal situation. The diversity of the social, political and economic landscape among the countries can shift this quickly. An example could be that workers of certain qualifications are very much welcome. However, members of certain groups of society would be viewed reluctantly, and so rather should be prevented from travel.

Also, internal stakeholders (see figure 2 and section 80: “Stakeholders”) can object to such plans. For instance, issuing visas can be an important revenue stream for the immigration agency or foreign office. They could see funds disappearing and so a loss of influence and options.

A quite extensive, but not exhaustive listing of topics for potential harmonization is listed in the check-list table 2 “Checklist with fields potentially subject to harmonization” in section 25: “What are key areas for harmonization”. Many of these topics are interconnected, and have a fundamental impact on national regulations and law. Again, it is wise to be sure that the objectives chosen are valid, and the instruments envisaged are really instrumental to achieving these objectives.

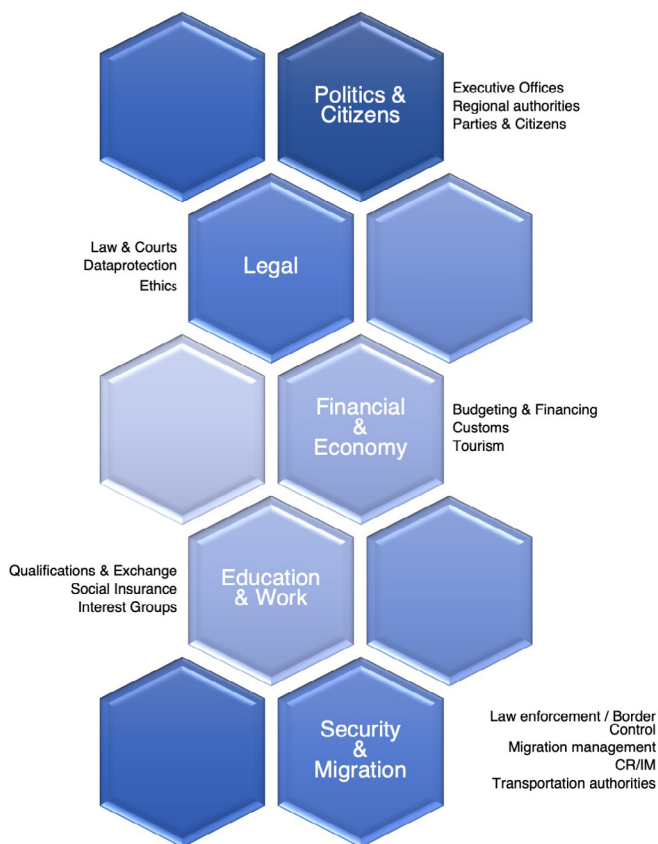


Figure 2 – Stakeholder groups for consideration in the process. A more detailed listing is provided in section 80: “Stakeholders”.

24. Establishing political will and operational engagement

Making an announcement for public consumption is the easy part of the process. A good part of diplomatic effort will be required to achieve the implementation of a joint working group for the evaluation and implementation of a free travel zone. However, embarking on the mission and actually driving the project into implementation and operation, is most challenging. Be aware, that depending on the extent of such protocol, such a project can well take several years or even more than a decade.



Path towards the European Schengen Treaty

As early as December 1974, the idea of a 'passport union' was born at the meeting of the heads of state and government of the EC Member States in Paris. The idea of a passport union was linked to the abolition of border controls. The basic idea behind this was also that the harmonisation of national passports would strengthen a sense of community.

By two Council of Ministers decisions (of 23 June 1981 and 30 June 1982) the Member States agreed to standardise the external form of passports by 1985.

On 25/26 June 1984, at the Fontainebleau Summit, the Heads of State and Government adopted eight texts modifying the Treaties of Rome and another on political cooperation. Taken together, they resulted in the Single European Act (hereafter SEA for short), which opened the way for further development of European integration. Among the most important points of the SEA are the realisation of an internal market free of all obstacles and a necessary and indispensable improvement of the decision-making structure of the EC.

In Article 14, the Treaty of the European Community, the SEA established as an objective the abolition of border controls, which was to be achieved in the Community by the end of 1992 at the latest.

The European Council also set up an ad hoc committee, also known as the 'Adonnino Committee', to examine measures to eliminate police and customs formalities at intra-Community borders for the movement of persons as quickly as possible. In the two reports of this committee, it named on the one hand measures to be realised in the short term, such as facilitating border controls or improving conditions for freedom of movement and residence, and on the other hand also longer-term goals. These included special citizenship

rights, culture and communication, youth and education, and strengthening the identity of the community.

The first concrete step towards the abolition of identity checks was realised by Germany and France in 1984. On 13 July 1984, they concluded the Saarbrücken Agreement, where they agreed to facilitate interstate travel. At the end of that same year, Belgium, Netherlands and Luxembourg agreed to this protocol, too.

Following the example of the Saarbrücken Agreement, Belgium, Germany, France, Luxembourg and the Netherlands sign the Schengen Treaty on 14 June 1985. In the years after 1985, it became clear that the Schengen states had vastly underestimated the difficulties in implementing the accompanying measures.

Main points concerned:

1. the intensification of police cooperation,
2. the establishment of uniform regulations for entry and control at the external borders
3. harmonisation of visa policy and
4. joint measures to combat drug trafficking.

This required improved cooperation between the judicial authorities in criminal matters, in the extradition of criminal suspects and illegal entry, and also the establishment of a joint computerised search and information system.

It wasn't until 1990 that the Schengen Implementing Convention (also called 'Schengen II') that the actual implementation and the operational cooperation among the authorities could take off.

European Commission (1985): Report from the ad hoc Committee on a People's Europe,
<https://ec.europa.eu/dorie/fileDownload.do?docId=186651&cardId=186651>



SUCCESSFACTORS



The above example of one of the most successful free travel zone, demonstrates the level of political will required. It must be deeply linked into the multilateral programmes, and not just to one presidency.

Key factors for a successful implementation evolve around these three points:

- organization-wide ownership and commitment to change;
- regular and effective prioritization, and;
- deployment of the right resources and capabilities.

25. What are key areas for harmonization

Harmonization is the action or process of making something consistent or compatible. In the context of free travel protocols, we would consider regulations, policies, laws, but also the looks of a travel document to be aligned.

Harmonization sounds like a very nice, smooth thing to achieve. However, it means that the parties involved need to agree to change their own views and even traditions in order to bring all the loose ends together.

In section 35: “Decision on interoperability and use of standards” we will take the discussion on harmonization a step further and look into international standards with respect to harmonization of the identity documents.

CHECKLIST



Fields potentially subject to harmonization (depending on objective and scope of the free travel protocol)	
Project Management	
<input type="checkbox"/>	The objective of the free travel protocol, as well as the roadmap.
<input type="checkbox"/>	Common project management approach, both for technical and administrative matters, combined with defined powers of decision.
<input type="checkbox"/>	Common time-line for individual phases of enacting decisions.
<input type="checkbox"/>	...

Border Management and Law Enforcement	
<input type="checkbox"/>	Law enforcement procedures (strategic and operational).
<input type="checkbox"/>	Common policy concerning the entry, movement and expulsion of foreigners (regular and irregular migrants incl.) and transfer of control of persons to the external frontiers of the Community. This includes agreements with third countries on expanded cooperation in frontier passages.
<input type="checkbox"/>	Proceedings with convicted criminals, both from Member States and third countries.
<input type="checkbox"/>	Common symbols of the Community's identity, including passports and ID-documents.
<input type="checkbox"/>	Documents to be considered for harmonization within the free travel protocol.
<input type="checkbox"/>	Security and layout of documents.
<input type="checkbox"/>	Combating drug abuse and crime.
<input type="checkbox"/>	Simplification of controls at frontier posts at mutual borders, while establishing common strategy on outer-frontier posts. Including the use of technology, the border control activities at the frontiers as well as within the territory (Remember air-, terrestrial- and sea-frontiers.
<input type="checkbox"/>	Structure of constant exchange among the specialist agencies of the countries involved.
<input type="checkbox"/>	Working migrant policy.
<input type="checkbox"/>	Visa Policy for members of third countries and residents of foreign countries.
<input type="checkbox"/>	Exchange of criminal records, nationality and vital events databases.
<input type="checkbox"/>	...
Economy	
<input type="checkbox"/>	Common taxation policy for citizens and goods, including forms and declaration numbers of goods, as well as tax exempt limits, especially upon relocation of private households. In general: avoidance of double taxation.
<input type="checkbox"/>	Taxation policy of persons working in one country and living in another, especially when living close to the inner-frontiers.

<input type="checkbox"/>	Tourism: Joint marketing and procedures for tourism in the whole Community, also considering multi-language support in the destinations.
<input type="checkbox"/>	Free movement of goods and money, irrespective of moved by the citizen, whether as a trader, professional man, worker or tourist.
<input type="checkbox"/>	Common market without tariff barriers, both for professional trade, as well as for citizens relocating.
<input type="checkbox"/>	Handling of exchange rate or currency effects among the Member States.
<input type="checkbox"/>	Social security procedures, when funds are collected in another country than in the country of retirement or health care is required.
<input type="checkbox"/>	...
Citizen engagement	
<input type="checkbox"/>	Simplification and reduction of the burden of Community legislation on the individual citizen.
<input type="checkbox"/>	Education and communication with the citizens facilitating them to understand the impact of the treaty and how to operate within.
<input type="checkbox"/>	Improvement of citizens' complaints procedures.
<input type="checkbox"/>	...
Citizen rights	
<input type="checkbox"/>	Voting rights.
<input type="checkbox"/>	Health and Social Security procedures.
<input type="checkbox"/>	Common emergency / call-for-help numbers, in case of emergencies and accidents.
<input type="checkbox"/>	Education field, especially recognition of diplomas and professional work certificates.
<input type="checkbox"/>	Youth and professional exchange programmes.
<input type="checkbox"/>	Handling of vital events in a member country other than the country of origin. This involves both policy as well as technical solutions.
<input type="checkbox"/>	Right of residence and work: extent of freedom of travel/movement, their families and personal goods within the community.
<input type="checkbox"/>	...

Table 2 – Checklist with fields potentially subject to harmonization

CHAPTER 6

WHAT TOPICS NEED TO BE HANDLED



As a consequence of establishing a Free Movement Zone, certain aspects that impact the entire FMZ have to be taken into account and consensus on these are necessary. One important aspect is Border Control Policy. States that are part of an FMZ need to have a uniform policy across all the members.

What you will learn about in this chapter:

- Issues to consider when designing the Border Control Policy
- The need for enhanced co-operation between members of the FMZ

26. For which user groups

An integral part of border management is the classification of travellers that enter or leave the country. When implementing a Free Travel Zone, it needs to be agreed on who the intended beneficiaries for the free travel will be. Below you will find a high-level selection of possible groups to consider:

CHECKLIST



Possible beneficiaries of <u>FMZ</u> border crossing (depending on objective and scope of the free travel protocol)
<p style="text-align: center;">Citizens and Residents</p> <p>Citizens and residents are subject to less inspection at Port of Entry or Exit. They tend to have preferential treatment in the inspection process.</p>
<p style="text-align: center;">Diplomats</p> <p>People representing a foreign country or nation or intergovernmental organisation are granted privileged access at the port of entry.</p>
<p style="text-align: center;">Business Visitors</p> <p>Foreign nationals who have a potential economic impact on the country. In most cases, these travellers carry a visa that designates them as a business traveller. They also tend to be frequent visitors to the country and hence sufficient advance information about them is known.</p>
<p style="text-align: center;">Tourists</p> <p>Foreign travellers who are a source of income for the destination country. The majority of these are not frequent visitors and not enough information about them is known.</p>
<p style="text-align: center;">Social visitors</p> <p>Typically, family members and relations of citizens and residents who come to visit. Their immigration status is linked to the existing citizens or residents.</p>
<p style="text-align: center;">Workers</p> <p>In many economies, people live in one country and cross the border to another country on a daily basis for work. Such crossings may also happen for informal cross-border trade. Migrant workers will resettle in another country, due to the working situation.</p>

Table 3 - Checklist of potential beneficiaries of FMZ border crossing

27. Common visa policy

FMZs must also determine if freedom of movement applies to visitors from overseas (e.g., outside the FMZ's member countries). If such freedom exists, then it would make sense to have a common visa policy. The key question to answer is whether a visa issued by a single member is valid across the FMZ or does a traveller need to obtain a visa for each of the members of the FMZ in case she wishes to travel within the FMZ.

FMZs are usually set up for economic reasons. A prime economic driver would be business travel and tourism. Allowing a traveller to cross borders within an FMZ based on a visa issued by a member country helps facilitate such travel and benefits the entire FMZ.

Visa policies lay out the eligibilities and considerations before issuing a visa to the foreign traveller.

If the members of a Free Movement Zone have different considerations of eligibility, travellers may try to obtain a visa from a member that has the least restrictive requirements and least number of checks on eligibility. Harmonising this process is therefore a crucial success factor for FMZs. If these are not harmonised across the FMZ, then the danger of 'visa shopping' exists.

Visa shopping refers to where a person may have been rejected by one member country, but then approaches another country to get a visa. To prevent such abuse, a common Visa Information System should be in place to allow Member States to check any interaction that the traveller may have had with any other member state and any background checks that may have already been carried out.

The EU Visa Information System (VIS) is an example. The VIS allows Schengen States to exchange visa data. It consists of a central IT system and of a communication infrastructure that links this central system to national systems. VIS connects consulates in non-EU countries and all external border crossing



points of Schengen States. It processes data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area. The system can perform biometric matching, primarily of fingerprints, for identification and verification purposes. It fights abuses, protects travellers, helps with asylum applications and enhances security. To learn more about this system, check the below referenced resource.



https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/visa-information-system_en

28. Common border management policy

In many economies, people tend to live in one country and cross the border to the other country on a daily basis for work. Such crossings may also happen for informal cross-border trade.

Travellers from outside of the FMZ will also use these borders.

STRATEGIC FRAMEWORKS

Establishing a common border management policy requires formulated common objectives and strategy in order to obtain such objectives. An integral part of this is a harmonized (or at least aligned) legal framework, providing authority to operate accordingly and in a coordinated manner. As borders always mark a touchpoint of two authorities, pan-national organizational structures and relationships are instrumental for successful operations, especially when it comes to preventing and fighting crime. Finally, the systems framework uniting processes and the IT-systems need to be covered.

One of these systems is an entry/exit system:

ENTRY EXIT SYSTEMS

To fight fraudulent behaviour of travellers, having an entry/exit system is a necessary part of effective border management. The entry/exit system allows the state to record the movement of travellers as well as to enforce a refusal of entry. It is necessary to prevent fraud such as overstaying a visa and involvement in criminal activities.

If the travel within the FMZ still involves border crossings, then each member state can manage their own entry/exit systems.

However, if the travel is borderless, then a common entry/exit system is required, as the traveller may enter the FMZ in one member state and depart from another.

The inclusion of travel history database functionality in their national border control system is a sovereign matter for States, and is therefore not the subject of ICAO Standards and Recommended Practices (SARPs). Interoperable applications such as Interactive Air Passenger Information (iAPI) and the Passenger Name Record (PNR), can be leveraged to create more complete and more accurate travel history databases.

Canada and the US have a joint entry/exit initiative between the two countries. The objective is to obtain accurate and objective entry and exit information from the border service agencies to support the administration of Immigration, refugee admissions and citizenship. The system helps verify residency requirements, investigations as well as status applications by family members seeking to emigrate.



More information on the setup can be found in below references

- <https://www.canada.ca/en/immigration-refugees-citizenship/corporate/publications-manuals/operational-bulletins-manuals/service-delivery/entry-exit.html>
- ICAO TRIP Guide on Border Control Management, 2018, page 54



29. Intelligence and data exchange

Information and data exchange is a critical component of an FMZ. This can include information on fraudulent documents detected, undesirable travellers (through exchange of watch lists), fraud patterns and criminal activities, lost and stolen travel documents etc.

It would be best to have a common repository of such information, but that would require a common processing centre that is hosted centrally. If the FMZ does not have such a common infrastructure, a bilateral exchange mechanism between members needs to be established at the very least.



Aspects recommended for consideration in this context:

OSCE-ODIHR (2021): “Border Management and Human Rights: Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context”, Warsaw, ISBN 978-83-66690-31-8, Available from <https://www.osce.org/files/f/documents/f/a/499777.pdf>

30. Granted rights

Freedom to travel may have associated limitations. For example, a traveller from a member country may enter any other member state, but has a maximum limit on the number of days he can spend in that country. There may also be restrictions on the types of activities they may engage in, like employment, studies etc. These need to be clearly articulated as a common policy among the members of the FMZ.

The rights that may or may not be granted are:

- Right to enter without a visa – There may be limits on the number of days that the traveller may stay in the destination country.
- Right to abode – FMZs may allow citizens from any of the Member States to live anywhere they choose or additional authorizations may be required.
- Right to study – special considerations may be given for students to enrol in an academic institution without requiring additional authorization.
- Right to work – The FMZ may allow free mobility of people to work anywhere within the FMZ or it may still require additional authorization from the destination country.
- Right of abode for dependents – If a person is working in a different country, the treatment of their dependents needs to be harmonized.
- Right to acquire and transfer property – Whether a citizen of one member state can acquire property in another state where he has the right of abode.

This is not an exhaustive list. It is intended to stimulate discussion on the rights that need to be harmonised and a consensus reached.

31. Leadership and ongoing monitoring

“ I figured something out. The future is unpredictable.”

– John Green, *An Abundance of Katherines*

An FMZ is a living entity. It needs constant monitoring, fine tuning and reacting to changes in circumstances. This is a continuous process and a mechanism to review and monitor the state of the FMZ must be established up front. Read section 24: “Establishing political will and operational engagement” and section 23: “How do you find a minimal common interest and anticipate blocking points” for some additional key-guidance.

32. Which ports/border-crossings are to be considered

Effective design of a Free Movement Zone strategy depends on the modalities of border crossing that are possible for entry to and exit from the country.

The type of traveller and the treatment of the traveller often depends on the modality of the border crossing.

Travel into and out of the country is done by air transport. This is the most prevalent and well documented form of border crossing and extensive literature of how to handle such a crossing is readily available. Many tools and standards exist for pre-departure clearance, advance information exchange and post arrival clearance. However, this may not necessarily be the modality which has the greatest number of travellers.

AIR PORT OF
ENTRY

For Regional Economic Communities (RECs), the majority of travel is expected across land borders. These may take the form of any one of the following.

LAND PORT OF
ENTRY

- Physical land borders – travellers cross the border through a physical checkpoint either on foot or in a vehicle (car, bus etc).

SEA PORT OF ENTRY

- Trains – It is also possible that such crossings are affected by transport mechanisms like trains that cross international borders.
- Informal border crossings – For countries that share a long border with their neighbours, crossing may occur at points along the border that are not necessarily designated as border crossings.

Primary transport is over water. This could be cruise ships or ferry crossings between neighbours or internationally.

Different considerations exist based on which port/border crossing is used by majority of citizens of the FMZ Member States. For example, if most of the border crossing is over the land border and very few crossings use the Air Port of Entry, then the focus should be on considering the consequences of establishing an FMZ mainly on the land border, like differentiated lanes for members of the FMZ. It is important that this exercise is done early in the process of establishing an FMZ.

33. Establishment of citizenship

One aspect that is usually left to the discretion and sovereignty of the individual Member States is the process by which the entitlement to citizenship is adjudicated. Each member state would already have in place, the process by which a citizenship application is processed. In all the current implementations of FMZs, this aspect is not harmonized.

However, these can lead to some issues:



There are some countries that allow citizenship by investment. Such citizens will enjoy all the rights of the Free Movement Zone. It has been noticed that people who would not qualify for a visa to enter one of the Member States, buy a citizenship from another state and are able to enter all the members of the Free Movement Zone. This can lead to conflicts between the members of the FMZ.



<https://investmentmonitor.ai/analysis/citizenship-for-sale-how-investment-buys-passports>

34. Dispute resolution

“ No matter how thin you slice it, there will always be two sides. ”

– Spinoza

While consensus may be reached before the establishment of the FMZ, there has to exist a mechanism for resolution of disputes that may arise from non-compliance by a member state or situations like the sale of citizenship by a single member state.

The following are a few examples from existing Free Movement Zones.



- The Court of Justice of the European Union is the judicial branch of the European Union and oversees the uniform application of European Union Law in cooperation with the national judiciary of the Member States. It is tasked to review the legality of the actions taken by the EU's institutions, enforce compliance to the obligations under the treaty, and interpret European Union law.
- The Caribbean Court of Justice is the judicial institution of the Caribbean Community. It is an international court with compulsory and exclusive jurisdiction in respect of the interpretation of the Treaty of Chaguaramas which established the Caribbean community.
- The COMESA court of justice has precedence over national courts and determines the legality of any act, directive regulation or decisions of any Member States.

These are just examples of the dispute resolution mechanisms being adopted by existing FMZs. It is important that such dispute resolution mechanisms be agreed upon and implemented as part of setting up an FMZ.

35. Decision on interoperability and use of standards

While the design of the identity document happens to be possibly the easiest part of harmonization, due consideration needs to be given to the emotional aspect of this exercise.

In designing a document, states rely on points that project national pride when choosing the language to be used, symbols, colors, crests etc. These are done with a view to showcasing the highlights of the country that this document represents.

However, when designing a common document for a Free Movement Zone, the design is no longer driven by the competence of national designers alone. Language, data fields, symbols, colors and crests, the layout itself, the definition of applicable standards (see below) and the production techniques can be made subject of mutual regulation, limiting one's own preferences.

On the up-side, harmonization of the documents leverages the feeling of 'belonging together' and presenting a unified front.

It can facilitate better processing and create economy of scale when procuring required infrastructure. On the down-side, it can create additional cost when production is done in diverse national facilities not equipped with the same technology. Also, it can lead to a lowering of security standards so that all members can produce the harmonized document. In the case of involving several manufacturing facilities, the arising deviations from the ideal harmonization can have an impact on security. Whether this is for the better or the worse, can be debatable.

WHAT ARE STANDARDS

A step beyond regional harmonization, discussed above in [section 25: "What are key areas for harmonization"](#), is the subject of international standardization. Perhaps we start off with clarifying what standards are. This term is regularly seen with various meanings. We look at it as a norm, convention or requirement. It could be a norm that is developed and applicable in a specific region. However, we focus here on international standards, which make them suitable for worldwide use. The international standardization body [ISO](#) defines: "A technical

standard is an established norm or requirement for a repeatable technical task. It is usually a formal document that establishes uniform engineering or technical criteria, methods, processes, and practices.”

Such standards could be about making a product (like the actual ID-document), managing a process, delivering a service or supplying materials – standards cover a huge range of activities.

Standards are the distilled wisdom of people with expertise in their subject matter and who know the needs of the organizations they represent – people such as manufacturers, sellers, buyers, customers, trade associations, users or regulators.

They can cover quality management, security management or IT security standards, just to mention a few areas that could be of interest to us in this guide. While we could discuss procedural standards, better called ‘best-practices’, we will be focusing on technical standards.

Standards could be considered being intrusive and cutting the degree of freedom. All countries and companies have brilliant minds that can figure out performant, custom-tailored solutions. So, following standards could be considered cumbersome, boring, not even well-fitted at first sight.

However, it could exactly be this reduction of variables, that will boost your project, letting it gain momentum quickly. This is even more so the case, when you need to work with various teams from different disciplines and even countries.

Trusted cross-border identity attestation is increasingly vital in today’s world. The ePassport is a fantastic global success story in this regard. This success is founded on the standards and specifications of ICAO who have put technical standards from ISO into a useful framework for international travel. Harmonization of content and format and inclusion of globally-trusted security features breeds understanding, convenience, usability and trust. As identity becomes more digital and the world more interconnected, future success will surely rely on international standards as for passports and ID-cards.

WHAT DO
STANDARDS DO
FOR ME

INTEROPERABILITY

Interoperability is a characteristic of a product or system, whose interfaces are completely understood, to work with other products or systems, at present or in the future, in either implementation or access, without any restrictions. Following well-chosen standards, defining this selection within the multinational project group forms the cornerstone of interoperable systems and a purposeful roadmap.

RECOMMENDED STANDARDS TO BE CONSIDERED



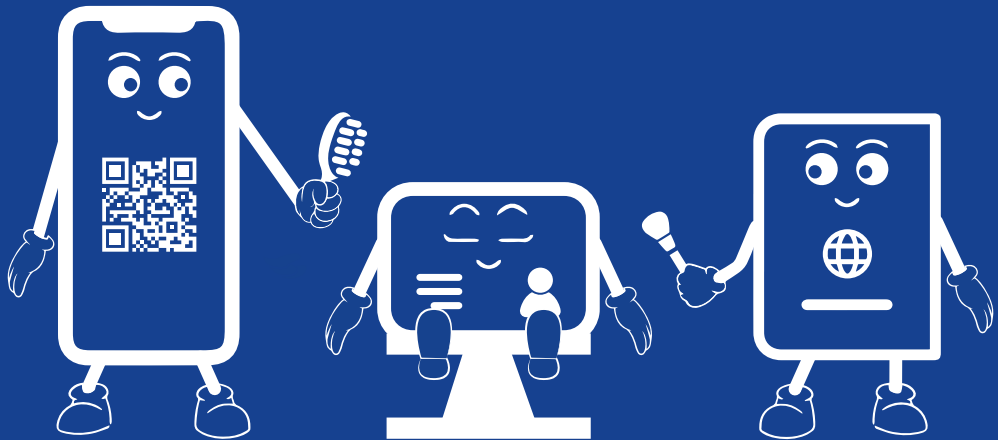
The following list is selective and non-exhaustive. However, it is intended to provide an entry point to this subject:

Management

- [ISO 2700x](#) “Information Security Management System”
- [ISO 14298](#) “Management of security printing processes”
- Documents
- [ISO 19794 / ICAO Doc 9303](#) “Machine Readable Travel Documents”
- [ISO 7810](#) “Identification cards — Physical characteristics”
- [ISO 7816](#) “Identification cards — Integrated circuit cards”
- [ISO 14443](#) “Identification cards — Contactless integrated circuit cards — Proximity cards”
- [ISO 39794](#) “Information technology — Extensible biometric data interchange formats”
- [ISO 19794](#) “Information technology — Biometric data interchange formats”

PART III

DESIGNING THE CREDENTIALS





INTRODUCTION TO THIS PART

Part 3 deals with [Theme B](#) mentioned at the beginning of this guide. It is intended as a short introduction to the technological aspects of issuing an identity credential which could either be an identity document or a travel document.

This part guides you through relevant aspects in selecting the most suitable document types, personalization technologies and document design. After having worked through these chapters you will have a basic understanding of various options, their characteristics and some dependencies.

Some of the concepts discussed here, require a basic understanding of the underlying technologies. A slightly detailed dive into further technological fundamentals is provided in [annex 1: "Some technological fundamentals"](#).

CHAPTER 7

SELECTING THE CREDENTIALS FOR FMZ TRAVELS



What you will learn about in this chapter

- Selecting the most suitable set of credentials for the specific FMZ-situation
- Designing the credential to meet the functional and non-functional requirements
- Where to find additional supporting resources

36. Which credentials could be considered for FMZ travels



Most travel within Regional Economic Communities (RECs) still involve passports. The usage of ID cards for travel within the REC is most prevalent in the European Union (EU).

The EU has a long history in the issuance and use of identity cards. Historically, centralized databases of citizens have proven problematic and hence there is a general aversion to having centralized registers of citizens that are accessed by providers of services to citizens. Hence, an identity card, which serves as a self-sovereign token has been widely adopted within the EU, and it serves as a replacement for centralized registers.

Few other countries have a tradition of identity cards. A notable exception is Brazil, with a broad range of physical and digital identity and legitimation cards, which is driven by their federalized structure. Some countries in LATAM have made some progress in having a single national identity card, but these are few in number.

In CARICOM, ID cards are issued by some countries. However, to date there is no harmonization standards for them. ID cards are one means out of several acceptable documents for inter-regional travel.

In Africa, identity cards are, to date an exception rather than the rule. A lot of effort is being put into establishing or modernizing the civil registries and centralized databases for holding citizen information. This can be seen as a prerequisite for a reliable national and cross-border identity management. The candidate list for suitable document types is very long, and in principle there are no limits to the imagination. In general, to be the most obvious, all documents already in use in the country are conceivable: birth certificates, school diplomas, voting and military cards, driving licences, etc. However, it should be borne in mind that what is a recognised document and issuing process in one country may be completely unsuitable for their processes in a second country. Therefore, we would like to outline three categories of documents:

1. internationally accepted and standardised travel documents (MRTDs);
2. national ID documents with bilateral agreements;
3. new technologies.

The choice of the preferred document type or document family is more than a decision on whether you want a glass of wine, beer or just fresh spring water today. The documents often differ in the requirements for the issuing or production process, the support of border management technologies as well as the space for visual data. We will discuss these criteria below. But first we will introduce different types of documents here.

So here we go with the first category: **The internationally accepted and standardized travel documents**. They are often referred to as Machine Readable Travel Documents. The International Civil Aviation Organization, a UN agency (ICAO), uses the acronym MRTD for these. This category comprises Passport-Booklets, ID-Cards and VISA-stickers.

ID-Cards have the typical format of credit cards, so called ID-1 format. Their visual data-structure follows a clear guideline, with some room for national specifics on the verso. They are readable by optical machine readers, so called OCR-B readers. This allows to capture key data from the document. However, there are also the options for adding contact- or contactless chips or even both interfaces. They are issued as National ID-cards, seafarer-cards, crew-member cards. Many countries have chosen to issue other documents of national use following this standard to a certain extent.

ID-CARDS

Passports consist of a) a cover, defining the type of passport, b) a data-page with the personal-identifying data and c) the visa-pages. They are both visually machine readable, as well as containing a contactless chip containing biometrical and biographical data. This document type is more than double the size of the cards mentioned above, a format known as ID-3. Also, they are typically at least three times as thick.

PASSPORTS

VISA-STICKERS

A visa is a conditional authorisation granted by a country to a foreigner allowing him or her to (ask to) enter, stay in or leave that country. The IOM Glossary defines a visa as “an endorsement by the competent authorities of a State in a passport or a certificate of identity of a non-national who wishes to enter, leave, or transit the territory of the State that indicates that the authority, at the time of issuance, believes the holder to fall within a category of non-nationals who can enter, leave or transit the State under the State’s laws”⁶.

Visas can typically include restrictions on the length of stay of the foreigner, the areas within the country they are allowed to enter, the dates of entry, the number of visits allowed, or a person’s right to work in the country. A visa usually takes the form of a sticker that is affixed to the applicant’s passport or other travel document.

STANDARDS AND RESOURCES



Standard References

Document type	ICAO	ISO/IEC
Cards	9303-5	7810/7816
Passports	9303-4	
VISA-Stickers	9303-6	

The ICAO documents can be found on the Webpage of ICAO:

<https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>

NATIONAL DOCUMENTS

The second class are **national documents that would be approved for travel by bilateral agreement**. Various documents can certify identity, nationality or the right to abode. If executed with sufficient identifiers and security, they could be used alone. In other cases, a collection of documents might be considered sufficient to prove identity and associated rights.

The challenge of using purely national documents, that do not follow any standardisation, is the lack of interoperability

⁶ IOM International Migration law - Glossary on migration, 2019, https://publications.iom.int/system/files/pdf/iml_34_glossary.pdf

for processing by neighbouring authorities. The need for coordination regarding form-factor, design, issuance process, but also verification of personal data is high.

The exchange of specifications, samples and operational communication channels between competent bodies to clarify uncertainties is central to safe management.

The **third class are the new technologies**. In this group we would like to list new document types that are in the process of international standardisation. At the time of writing this guide, these are not yet final, but are being used nationally. They are therefore options for international interoperability.

Here, mobileID can be considered, which are applied in particular for mobile driving licences. Likewise, Visual Digital Seals (VDS) as a technology that can be used mobile or printed on physical documents.

Digital Travel Credentials (DTC).

DTCs are a new class of technology under consideration. They allow for the travel document to be in a form factor that is different from a booklet. For example, a credential that is held and is visible on a 'smart card' or a mobile phone. The DTC is defined as having a Virtual Component (VC) and a Physical Component (PC) and are intended, at least initially, to complement the eMRTD.

Visible Digital Seal (VDS)

A Visible Digital Seal is a Digitally Signed 2D barcode that can be used to protect non-electronic documents. For example, Visa stickers and Emergency Travel Documents. The VDS is being used in the Schengen Visa sticker to protect the integrity of the visa and to detect forgery or tampering

Visible Digital Seal for Non-Constrained environments (VDS-NC)

The VDS that we mentioned previously is optimised so that it does not take up too much space on the visa sticker. As a result, it has limited data carrying capabilities.

For situations where size is not a big issue, ICAO has defined VDS-NC. Furthermore, two profiles using VDS-NC have

been specified. One if for Covid Proof of Testing (PoT) and for Covid Proof of Vaccination (PoV). More recently, a profile has also been defined for Digital Travel Authorization (DTA), which is effectively an eVisa.

37. Considerations on place of issuance and personalization

In section 36: “Which credentials could be considered for FMZ travels” we looked at form factors of credentials, what they look like and how their intended use varies. Before jumping into the subject of technologies or specific systems, you need to evaluate your issuance requirements, and related to this where you will be adding the personal data to the blank documents (personalization).

Choosing the right form factor is not limited to the appearance of the document itself. Rather, the document is a product of various factors. Such factors include where these documents are to be issued, what waiting times are involved, security considerations for anchoring personal data as well as their colour, the longevity of the document and how these documents are to be operationally integrated into the business processes of the regulatory authorities.

Many of these factors have interdependencies, and involving knowledgeable staff or unbiased consultants to guide through the options in identifying the most suitable way should be considered. Still, let us take an entry-level look at some of these aspects:

ISSUANCE & PERSONALIZATION TOPOLOGY

Being close to the citizens and offering good service is key for the success of programmes. In this context, we need to consider three steps: The place of (1) enrolment, (2) production and (3) issuance of the documents.

As part of the enrolment processes there are the following steps of:

- validating primary data;
- background checks, and;
- data preparation.

Depending on how these steps are organized and integrated into existing systems, you might be able to consider the on-the-spot issuance of the documents. Issuance on-the-spot helps considerably to reduce the burden on the entitled persons for receiving their documents.

Another option to achieve this reduction of burden is to offer full online registration-services, with preclearance. When on-site, the only steps remaining are to identify the person and to validate the authenticity of the foundational documents. In practice, this option can be considered when no biometrical data needs to be enrolled or is part of the background checks.

Looking into the personalization topology, we can differentiate four basic models:

Centralized Personalization

The first is centralized personalization. This means that data is collected from across the country and the physical documents are individualized with the personal data in batches at a central facility.

This method allows for the use of high-capacity machines, high logical and physical security measures, as well as best production situation such as business-resilience, power-management and climate. Also, the handling of system failures can be easily managed with proper redundancy planning.

It can be expected that the cost per piece will be considerably lower than with decentralized personalization.

However, waiting times and logistical challenges need to be overcome.

Furthermore, a strong business continuity management needs to be set in place. This means, having a second independent site of operation is crucial in handling the risk of full site-failure by critical utility failure or disaster.

Decentralized Personalization

Decentralized Personalization means the personalization right at the spot of registration. Also, it could imply 'over-the-counter' issuance.

Typically, the machines will be smaller than in the centralized case. The organization of issuance centres and associated costs, the requirement for secure storage, production management, data preparation as well as backup management need to be considered.

For all the personalization technologies mentioned in section 39: "Considerations for the personalization technology", machines suitable for decentralized personalization are available.

Normally, the total cost of personalization will be somewhat higher than in the case of centralized personalization.

However, the implications of logistics both for the government and for the applicants are the advantages of this kind of process.

Mobile Personalization

If people from remote areas cannot travel to the registration or personalisation centres, but the centres travel to the people, then mobile personalisation infrastructure is required. This can be an infrastructure in transport boxes placed in local offices. But in the best case, it can be actual specialised vehicles that provide both office space and technical work areas for personalisation and data transfer.

Depending on the implementation, the climatic situation, the energy and compressed air supply and the sensitivity to vibrations must be considered.

The involved costs will basically be comparable to decentralized personalization. However, the cost of building and operating the special vehicle will need to be compared to the cost of operation of a local office.

Special considerations need to be spent on the security and communication infrastructure.

Possible future developments: Online / Over The Air (OTA)

If the option of digital rather than physical documents is pursued, new aspects of personalization open up. For example, the future data carrier (e.g., a smartphone) or a user account can be uniquely registered when the application is submitted. This means that personalization can be carried out over the air (OTA) at a later date. This technology is being actively researched and standardised and may become viable in the near future.

38. Considerations for eMRTD issuance and personalization

If you choose to issue eMRTDs, some additional considerations apply.

If you do not have an understanding of the underlying technologies related to the issuance of eMRTDs, please refer to annex 1: “Some technological fundamentals” before continuing with this section.

The data in the chip has to be signed by a document signer that is issued by the Country Signer Certificate Authority (CSCA) of the country.

There are a few scenarios possible for the deployment of the signature function depending on the chosen personalization model

Centralised Personalization

In case the centralized personalization model is chosen, the deployment of the Public Key Infrastructure (PKI) and Signing infrastructure is quite straight forward. The CSCA and the Signing server are located at the same personalization centre.

Decentralized Personalization

In case of decentralized personalization, there are two options that are possible:

1. Centralized Signing – While the personalization can be done at the point of registration, the data would be sent to a central signature facility to create the Logical

Data Structure (LDS) and the Security Data Object (SOD). These would then be injected into the chip of the credential.

In this case, a secure connection between the remote personalization centre and the central signing server is required and proper authentication of the requesting entity needs to be managed.

2. Decentralised Signing – In this model, the document signer and the signing server are hosted at the same location as the personalization system.

The DSC keys are generated locally and then have to be transported to the CSCA for creating the Document Signer Certificates. The security of the transfer of the keys and the certificate needs to be properly planned and executed.

39. Considerations for the personalization technology

Selecting the personalization technology is based on several aspects. These aspects are:

- Security considerations: What kind of security features are possible with the specific technology? And how can the personal data be secured within the selected substrate?
- Total cost of ownership: Some technologies are costly on investment, but very cost effective in their operation. Others are vice versa.
- Circumstances of personalization: Where will you be personalizing the documents and what is the climate and utility situation in those places.
- Visual effects: The visual impression of the personalization can vary considerably. One of the most obvious differentiators is the desire for having colour portraits.
- Production speed: Both the technology as well as the machines have typical production speeds and capacities.

Below we will look into some of the most frequently used techniques and technologies:

Laser Engraving

Laser engraving is the use of lasers to inscribe or mark an object. This term is commonly used in the identification industry. More correctly, it should be called laser marking. This is because the laser marks an object with a colour change through chemical/molecular changes such as charring, foaming and melting. This technique does not use inks or tool heads, which come into contact with the engraving surface and can wear out.

Compatible substrates are polycarbonate, as well as specially prepared PVC and PET (see below).

On one hand there are no consumables besides the cards required, saving cost and easing the supply-chain. On the other hand, the investment in machines and the utilities (power, climate, perhaps pressured air) are in most cases higher than with other techniques.

Inkjet

Inkjet prints are created by sending computer data as an electrical signal to a printer, which converts the data into small droplets of ink that are sprayed onto a substrate in tiny droplets. The droplets are applied with variable spacing, density and size to produce a wide range of hues and shades. Compatible substrates are paper. When using security paper, there might be the need for a compatible surface treatment. However, there are specific ink and substrate combinations that will allow to personalize even polymer card bodies.

Toner Laser

Toner Laser belongs to Xerography, or electrostatic printing processes. Electrical charges and light are manipulated to fix toner particles in the form of an image or text to a substrate via a photoreceptor drum or a metal roller coated with light-conducting material. Toner is then applied to the surface of the drum. Dry toner consists of pigments or dyes suspended in thermoplastic resin particles.

The technique is suitable for paper or synthetic papers. Special processes can make it suitable for other substrates, too. The system is very cost effective and comes with a good longevity. However, the level of security achieved is disputable and needs more review than other technologies listed here.

Dye Diffusion Thermal Transfer (D2T2)

Dye diffusion thermal transfer (D2T2) is a digital printing process that uses heat to create a dye image in a substrate. Despite the name, sublimation is unlikely to occur during printing. The process is best described as diffusion. However, 'dye sublimation' is an often heard term for this technique.

This process uses ribbons, either in one colour, or as multi-segment ribbons. The personalization can be in colour and usually has a very high photorealistic quality. It is suitable with PVC, and can work with ABS and PET. Only in case of composite-cards, a Polycarbonate-cored card could be processed with D2T2, too.

The ribbons are a rather costly component of the document. Also, after their use, the waste contains personal data. This needs to be considered in the secure waste management. Also, this process comes with an adverse ecological footprint.

The application of the high quality, well suited holographic transfer foils are a prerequisite in order to achieve a minimum acceptable security level. Additionally, a protective patch should be considered, in order to resist wear and tear.

Handwriting / Typewriter

These very simple techniques might surprise in this context. However, special situations can require special measures, such as with the issuance of refugee documents, emergency passports and other. Generally, it is not advisable to allow these techniques, despite being very cost effective.

Digital-Printing

Digital printing can combine elements of pre-printed, static elements with dynamic, variable data. To a certain extent it

is related to the Inkjet and Toner-Laser printing described above. However, it is suitable for high-speed and high-volume production. Also, the printing quality is superior to the methods mentioned above. This process can disrupt the conventional process of preparing finished documents followed by printing the individual data. In this case, all elements are pre-printed, followed by a finishing process. It is suitable for centralized or high-volume regionalized production sites and can be very cost effective.

Compatible substrates are paper as well as PET. Rapid development progress is being made on Polycarbonate, too.

40. Considerations of the document material

Besides the choice of the document type and the personalization technology, the suitable choice of the material has an impact on the cost. Two dimensions need to be considered: the cost of procurement and processing, and the longevity of the document made of this material.

DOCUMENT MATERIAL

Types of plastics

Most popular materials used for cards are PVC and Polycarbonate (in short PC). Also, various PET derivatives and ABS blends are used. In recent years it has become more difficult to categorize the longevity of the documents, as the various derivatives and processing technologies can create considerable variations.

PVC (Polyvinyl Chloride):

Typically you can expect PVC to be suitable for rather short-term (2-4 years) and low-stress use-cases. This material is most often used in combination with Dye-Diffusion-Thermal-Transfer personalization technologies (see section 39: “Considerations for the personalization technology”). Likewise, this technology is suitable for rather short use cases. Therefore, you will need to reissue documents more frequently.

The cost of cards made of this material is low.

PC (Polycarbonate):

Polycarbonate is seen as the gold-standard for card-documents. When handled correctly, it has a very high robustness and a usual service life of 10 years and more. However, when exposed to sweat, softeners, heat as well as mechanical stress, its service life can be considerably shorter. The cost of documents made on basis of this material is in the premium segment. This is due to the material, the processing, as well as the high-quality security technologies that can be integrated. This material can be personalized using laser-engraving. When special treatments are applied, D2T2 and Inkjet can be used (see section 39: “Considerations for the personalization technology”).

PET (Polyethylene Terephthalate)

This material is applied in various formulations with considerable impact on its characteristics. In general, it is considered to be a rather eco-friendly material. The service life can be 5-8 years, in some cases even 10 years could be reasonably assumed. The document cost is positioned between PVC and PC. Depending on the specific formulation and build, a broad range of personalization technologies with their specific characteristics can be applied.

Card alternatives

Alternative builds for making card-based documents can be based on paper, security paper, plastic-coated papers or even synthetic papers.

When designing security documents, using office paper would have the lowest cost. However, the price lies in the system reliability and security. In general, this should be considered as a non-option.

Instead, the use of security paper could be considered. It contains numerous security features directly integrated into the substrate. It has a good robustness and can be thicker and more durable than usual paper, e.g., 300g/m². Especially synthetic security substrates can offer cost-effectiveness, good security and longevity for such documents, without the need of being pouched.

41. Considerations on data storage

Another decisive and functional element in selecting the credential is the factor for data storage on the credential itself. Supporting specific reading interfaces could make the use of standards advisable, which again can impact the type of credential. Others can set boundaries on the resilience to wear-and-tear, such as when reading data with swipe-readers. There are various options for mobile data storage, and often they can also be combined. Some of the options for making this data available in machine-readable form on the documents are presented here.

With all the options listed below, you can create a link for online database queries, in order to access dynamic, updated information.

OCR-B

OCR is an acronym for Optical Character Recognition. The 'OCR-B' is one of the versions defined in the ISO standards (ISO 1073-2). Its function is to facilitate optical character recognition by certain electronic devices, originally for financial and banking-oriented applications. While basically any scanner equipped with the optical character recognition algorithm can reliably capture the data, swipe readers used in airports and banks can do so very efficiently, too. The data density is low, and it is recommended to follow a strict data-block logic and introduce check-sums for error detection.

0 1 2 3 4 5 6 7 8 9
A B C D E F G H I
J K L M N O P Q R
S T U V W X Y Z <

Figure 6 – Subset of OCR-B Characters from ISO/IEC 1073-2 for use in machine readable travel documents (From ICAO Doc 9303)

A **QR-Code** is square and easy to recognise by its finding aids, nested light and dark squares in three corners. The symbol elements are squares, of which there are a minimum of 21×21 and a maximum of 177 × 177 elements in the symbol. There are four error correction levels that allow reconstruction in case of damage from 7 % (level L) up to 30 % (level H). More than 4000 alphanumeric characters can be encoded per code. Larger contents can be divided into up to 16 individual codes. The micro QR code accepts up to 35 digits.

In the **DataMatrix code**, the Reed-Solomon error correction adds redundant data. Between 30 % and 60 % of the code words are thus code words for error correction. This allows some erroneous modules to be corrected without jeopardising decoding.

The name **Aztec code** is derived from the advanced civilisation of the Aztecs in central Mexico and their step pyramids: If you look at a step pyramid from a bird's eye view, it strongly resembles the squares that can be seen directly in the centre of the code, centred around a single point. In the centre of the code is the search element, which consists of several nested squares. The symbol elements are also square. Small (from 12 characters) to large amounts of data (currently over 3000 characters) can currently be encoded. The content can be divided among several symbols. The Reed-Solomon error correction supports user-specific up to 32 security levels. Reconstruction of the data content is still possible even if up to 25% (for small codes even up to 40%) of the code has been destroyed. In contrast to all other codes, no quiet zones are necessary. The code can thus be placed at any desired location.

Visual Digital Seal (VDS)

The acronym **VDS** is defined by **ICAO** as a Visual Digital Seal. It is a cryptographically signed data structure containing document features, encoded as a **2D** bar code and printed on a document. As such, the **VDS** is a structured application of the **2D**-codes described above. The header contains information about the issuer, and the whole seal is digitally signed and so protected in its integrity and authenticity. By the application of

a standard data carrier and a standardized application of it, a reliable interoperability is achieved.

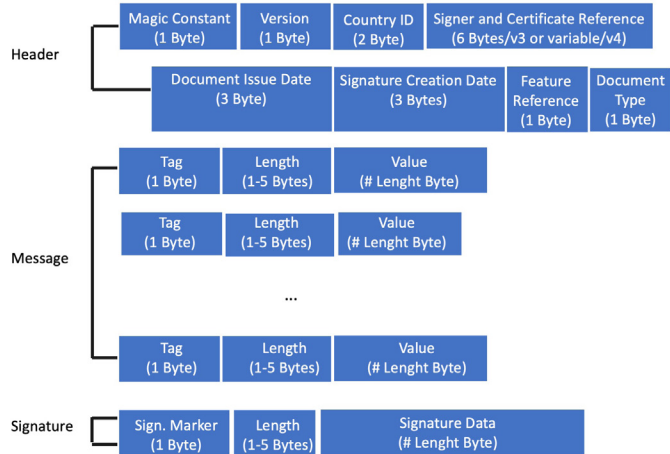


Figure 9 – Data elements in a visual digital seal (VDS); ©ICAO Doc 9303



If you consider this to be an option for your project, be sure to read up in this technical report on VDS.

<https://standart.aero/en/icao/book/doc-9303-p-13-machine-readable-travel-documents-part-13-visible-digital-seals-en-cons>

Visible Digital Seal for Non-Constrained environments (VDS-NC)

The VDS mentioned in the previous section is optimised for space as it is intended to be printed in a Visa sticker, which has space limitations. For situations that do not have space limitations, ICAO has specified the VDS-NC.

Similar to the VDS, it is cryptographically signed data structure, encoded in a barcode and printed on a document. The data payload is human-readable and the VDS-NC can be read by any barcode scanner.

The VDS-NC is specified for the following uses:

- Covid Proof of Testing – ICAO has specified a profile to use the VDS-NC for issuing proof of testing that is globally interoperable and can be verified offline.

- Covid Proof of Vaccination – ICAO has also specified a profile for encoding the vaccination status of a person in a manner that can be verified globally. The issues of this this proof will be the country where the person took her vaccines.
- Digital Travel Authorization (DTA) – DTA is the term that is used to denote visas that have been issued electronically without a visa sticker having been issued to the holder. They usually take the form of a PDF document or a printable image that the holder carries with them to prove their visa status. A VDS-NC profile has been defined for DTA to ensure that it can be verified globally and offline.

The technical reports are available at:

<https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Visible%20Digital%20Seal%20for%20non-constrained%20environments%20%28VDS-NC%29.pdf>

<https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Digital%20Travel%20Authorizations.%20%28New%29.pdf>

Chip technology (contact/contactless)

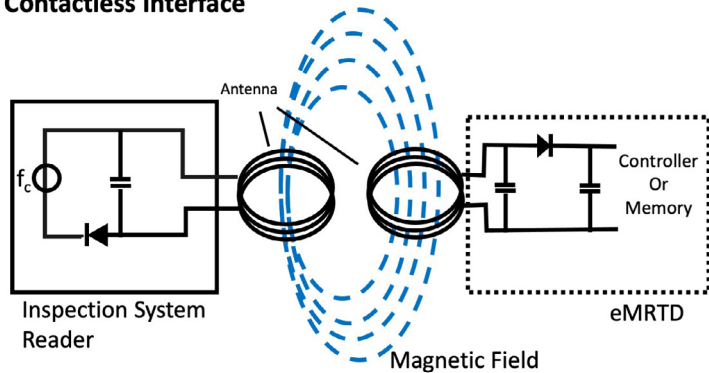
The use of chip technologies in ID and travel documents follows strict definitions set-out in ISO 7816, ISO 14443 and ISO 15693. These standards technically define how the chip can communicate with the surrounding systems. Generally, there are contact-/contactless- and dual-interface chip systems. Especially the contact-chips need to be placed at predefined spots on the card, in order to interoperate with the chip readers.

These chips can be simple ID or storage chips. However, they can range up to real crypto-processor multi-application microcomputers supporting advanced security protocols like Active Authentication, Chip Authentication, and when using additional biometrics: Extended Access Control. These terms will be explained to some extent in section 47: "Access control for biometrics" and section 63: "What are eGates"



The storage and computation capacity can vary strongly and are developing rapidly. Security certifications need to be considered, as they provide a level of trust for the specific application. These need to be considered, both at the time of procurement as well as during the service lifetime.

Contactless Interface



eMRTD chips are receivers, they use a load modulation technique

Figure 10 – Schema of the electrical functioning of a contactless Interface

42. Functional considerations for selecting the document

There are various aspects you will want to consider when deciding on the document to be used. But first of all, we should be clear, that there is no need to allow only one or two types. More important are the procedures behind the document and the security involved in its issuance and production. We will briefly touch this subject in chapter 16: “Linking of identities with people”.

Below a quick, but not exhaustive, overview of some important aspects:

SIZE OF DOCUMENT

You will want to have a good understanding of the visual data to be represented on the document. Making the font or graphical elements smaller has certain limitations. Therefore, you will need to choose between amount of data and the document type. In the order of increasing capacity in terms of visual data, you can work with cards → visa stickers → Passports → Certificates.

As an authority, you can impose a general obligation to carry the documents and regulate how they are to be used. The practical success of such obligation will in part depend on the extent to which you provide a practical form factor for the population to carry with them.

Passports tend to be cumbersome to carry around in general. In many cultures, the card is the preferred option. For populations that are technology-savvy and rather affluent, mobile data carriers or app-based solutions can find even greater acceptance. Physical certificates (documents) can be customised to specific use-cases and do not require infrastructure for storage such as phones or wallets.

When considering documents, the price of the document for the citizens is an important aspect. On one hand, the possession of such a document and the eligibility for the attributed rights should not be discriminating merely on monetary basis. On the other hand, as administration, you will need to consider the total cost of service.

Setting the price is influenced by its cost. Purely looking at the physical document would be distorting your decision. It is advisable to consider the total cost, including the technology for writing the individual information, requirements for secure and reliable operation. On the income side, you will want to consider if one document and its acceptance will drive other economic interests in favour of your balance sheet.

On this topic you will find some more detailed guidance in [section 39: “Considerations for the personalization technology”](#) and following sections.

Selecting the document type and technologies to implement them needs to consider the expected service life. Passports are typically issued for 10 years. Birth certificates are issued for a whole life. Visa-stickers are usually issued with validity from a few months to several years, just as ID-cards.

Be wary about generic claims from suppliers, as long as you have not defined the circumstances in which the documents will be used:

- Climate is one factor;
- Frequency of use and type of use, is another.
- What is the expected manner that population will be carrying the documents with them?
- Besides standardized tests for longevity, the actual use of the document is a concern: Is there a known abuse of the documents that impacts the lifetime of them and should be considered when specifying the requirements? Examples of this is using cards as ice-scrapers on windshields, or as screwdrivers.

ISSUANCE PROCESSES

The topic of issuance is another element in the security chain. Will you be issuing the credentials centralised or decentralised? We discussed this in more detail in [section 37: “Considerations on place of issuance and personalization”](#), and [chapter 16: “Linking of identities with people”](#).

Connected with this, consider live data-capturing versus scanning or online harvesting. Capturing the portrait photo is substantial. While biometric data-capturing (such as fingerprint or facial biometrics) requires a live capturing, the face is still often captured from supplied photographs. This allows the risk of photo manipulations, such as morphing.

A face-morphing attack is an attack on a biometric facial recognition system, where the system is fooled to match two different individuals with the same synthetic face image. Such a synthetic image can be created by aligning and blending images of the two individuals that should be matched with this image. Special attention should lie on the verification of ‘breeder’ documents. These are documents being presented as proof of identity and eligibility. When such documents contain digital data or links to online-data, you might want to be able to validate their authenticity and use the interfaces to import into your issuance system.

SECURITY OF DOCUMENT, VISUAL DATA, ELECTRONIC DATA

Security of the document and its data is a very central requirement. At the same time there is no absolute “yes” or “no”. Rather it can be answered in a level of resistance against attacks or types of fraud relative to the effort to accomplish the fraud.

Security comprises:

- the security features on the blank document;
- the securing of the personal data added to the document;
- logistics in transporting and storing the documents and their components;
- Human resources involved in all the steps of issuance, and;
- IT security.

You will need to find an adequate balance between risk and impact. Bear in mind, that security can create user-experience disruptions, which may result in reduced user acceptance or ‘creative security breaches’.

How are you intending to use the documents for border crossing and policing? When your intention includes to involve machine processing, you need to consider the suitability of the documents and the required interfaces.

SUITABILITY
FOR BORDER
CROSSING
TECHNOLOGY

Technology	Reader	Documents
OCR-B	OCR-Swipe Readers	Cards, Visa, Passports
2D-barcodes	Document scanners, Smartphones	Certificates, Cards, Visa, Passports, MobileID
Contact Chips	Card Readers	Cards
Contactless Chips	Document scanners, ABC-gates, (Smartphones)	Cards, Visa, Passports, (MobileID)

Table 4 – Matrix visualizing the connections between data-carrier technologies, required readers and suitable documents as technology carriers

How should the credentials support both domestic as well as partnering countries business processes at the border, as well as interact with other authorities such as labour, health, law enforcement. This subject is much broader than the traditional reflections on passports are considered. Many stakeholders might be interested, depending on the nature of the FMZ.

BUSINESS
PROCESS
INTEGRATION

The criteria ‘Inclusion’ has several dimensions to be considered. We will cover them later in section 49: “Considering special needs”. Here we discuss visually impaired, elderly and children. Credentials should not be discriminatory due to cost, or e.g., require pre-investments in a smartphone for all family-members. Also, they should be able to be handled by non-tech savvy persons as well as people living remotely with limited access to electricity or communication technology.

INCLUSION

CHAPTER 8

DESIGNING THE CREDENTIALS



What you will learn about in this chapter:

- What needs to be considered when designing the FMZ credential
- Aspects of harmonization and liberalization relative to data, design elements and security concepts
- Where to find additional supporting resources

43. Getting started when designing the FMZ credential

“ Sometimes the questions are complicated and the answers are simple. ”

– Dr. Seuss

While this check list might not be exhaustive, it still contains an important step-by-step approach to the process. This will only be an overview, and more details can be found in this guide, as we point out in the checklist itself.

CHECKLIST



Designing the FMZ credential	
<input type="checkbox"/>	Before starting designing the FMZ credentials, be sure that you have decided on the type of document. If you haven't done so already, be sure to read chapter 7: "Selecting the credentials for FMZ travels".
<input type="checkbox"/>	Decide on the level of interoperability required. This is important as it defines uniform data-formatting and technology elements to be integrated. In this context you will find yourself moving gradually into a more pre-defined layout design given by standards. Read section 35: "Decisions on interoperability and use of standards" and section 45: "Harmonized visual data-layouts".
<input type="checkbox"/>	Design clear use cases for each data field. This is important for several reasons: <ul style="list-style-type: none">• For privacy reasons. You should be clear on who would use this kind of information for what reason. And who could abuse it when the document is regularly presented, or even lost.• As part of the above point, you can define what will be humanly readable, what will be stored digitally, and what would be even cryptographically access-restricted or only accessible via online-link.• When the space on the document is tight, you can prioritize what information needs to be printed visually, or stored digitally.• A clear use case helps define rules that prevent variations in populating the field with non-supporting information.

<input type="checkbox"/>	<p>Define threat models, and possible responses to them. This serves to lay the foundation of the security concept. Think about organized crime, identity theft, illegal migration and work, customs fraud, etc. Check out the next section 44: “How do we design a harmonized security concept”. See the subtitle “Intelligent Security Concepts” for some more guidance.</p>
<input type="checkbox"/>	<p>Decide on the degree of uniformity of the documents. Provided multiple nations intend to issue a common document, you will be confronted with national interests and pride.</p> <p>Both the authorities as well as the public will want to have the feeling of the document representing their home land while having the sense of new multi-national opportunities.</p> <p>Governmental documents are a piece of identification with one’s origins. Where is the emphasis? Region or Nation? Thus defined emblems, choice of colours and ornaments designing a concept with both harmonized and localized layout elements is an important step. This consists of design elements, security features and data elements.</p>

Table 5 – Checklist: Preparing for the Design of the FMZ-credential

44. How do we design a harmonized security concept

Security of a document is not limited to the selection of the security features on the document alone. It is rather about the end-to-end process. It is this holistic view that will guide you in designing the credential with an adequate security concept. Earlier, we discussed various personalization techniques and security substrates. The following selection of questions can serve as a self-assessment or planning tool:

Harmonized security concept	
<input type="checkbox"/>	Has the design and specification of the document engaged all stakeholders?

SECURITY AS A
CONCEPT

CHECKLIST



<input type="checkbox"/>	Have all the elements been considered in a comprehensive and cohesive manner?
<input type="checkbox"/>	Have the manufacturing tolerances of print and assembly been considered?
<input type="checkbox"/>	Is the enrolment and adjudication process secure in itself?
<input type="checkbox"/>	Are biometrics being captured live and are images of the right resolution?
<input type="checkbox"/>	Has the personalisation system been security and volume tested?
<input type="checkbox"/>	Has a prototype document been checked for compliance?
<input type="checkbox"/>	Has the document been tested for durability and attack resilience?
<input type="checkbox"/>	Have the details of the new document been communicated to the relevant services, such as foreign border services, so that it will be recognised and accepted?

Table 6 - Checklist: "Designing a harmonized security concept"

SECURITY SPECIFICATIONS



For the security (feature) concepts, there are various guides available. Two samples, one from ICAO, and one from the European Union, and details are provided further below.

Both provide a set of security features to be used as a minimum. In most cases, these features are rather descriptive, not endorsing a vendor-specific solution. A sample of this is 'OVDs', or 'optically variable devices', including holographic elements and diffractive features made by other processes.

These recommended minimum standards focus on providing only a list of features. They do not provide guidance on how to use these features effectively. The focus of these lists rest on interoperability, and not so much on the achieved security per se. However, there are efforts from inter-industrial interest groups and working groups within the standardization bodies to provide better guidance on how to evaluate the efficiency of the applied technologies.

INTELLIGENT SECURITY CONCEPTS

When designing the document security concept, you will want to have prepared an assessment to the following topics:



Intelligent Security Concepts	
□	<p>What is the threat model?</p> <p>You might find answers by consulting your own and foreign documentation and statistics on counterfeits. These are important resources of learning how to design and improve.</p> <p>However, having low evidence of counterfeits can have very controversial consequences:</p> <ul style="list-style-type: none"> • In the best case, your documents are very secure. • It could also mean, that the incentive of counterfeiting isn't as high as other opportunities are. • On the down side it might be that your authorities are not inspecting the documents enough, due to lack of training, tools or leadership. • You may not know what is happening with your documents outside your area of responsibility. Think of international areas of use, or related use-cases (e.g. for banking transactions). • And finally: The documents might be so weak, that the counterfeits are perfect or the supply-chains are infiltrated.
□	<p>What are the characteristics of the selected substrate and personalization techniques?</p> <p>Consider the points described in section 39: "<u>Considerations for the personalization technology</u>" and section 40: "<u>Considerations of the document material</u>" and consult interdisciplinary specialists.</p>
□	<p>Who needs to be able to verify the authenticity?</p> <p>Very often document security concepts are designed to the needs and capabilities of the major ports of entry, namely the airports. However, the infrastructure and training at sea ports and terrestrial borders are often the weakest points. Even more so, when law enforcement and border management need to take place with police forces within the country perimeter.</p>

	<p>Finally, consider other public and private sector dependencies, such as civil registries, banks, sales offices etc. Their tools and training might be very limited, as well as their clearance for checking on a higher set of security technologies.</p> <p>Profiling the stakeholder inventory and their abilities and needs is key for an effective security concept.</p>
<p>□</p>	<p>How are the documents to be manufactured?</p> <p>In FMZs you might prefer to have the documents manufactured domestically. This results in multiple suppliers producing to a harmonized specification. Each process and machine have specific characteristics, and this will inevitably result in deviations. This might be a weakness. This can be turned into an advantage as documented and specified deviations can add a layer of security.</p> <p>When selecting the technology and designing the specifications, this is a factor to be considered.</p>
<p>□</p>	<p>Is the concept to be applied only for a single document, or a family of documents?</p> <p>Passports, but also ID-cards are issued as document families in some cases. Regular passports, diplomatic or service passports etc. are issued with differentiating design while mostly maintaining a similar security concept.</p> <p>When the place of personalization or issuance differ (often the case for diplomatic passports, or emergency documents), you might be confronted with seriously different technologies and circumstances. Taking this into consideration by an inter-ministerial working group can in the best case, avoid weakening the security concept.</p> <p>A second case of document families is given when both passports and cards are to be issued following the same security concept. Differences in substrates, document formats as well as personalisation technologies need to be identified and addressed.</p>

<p>□ Be forward looking. Absolute security is non-existent, both in the physical as well as in the digital world. Designing a security concept without a plan for future upgrades would be seen by many as naïve.</p> <p>While we don't know how and when breaches will occur, it is safe to assume that they will happen. When designing your documents, consider scenarios and prepare for upgrade plans. Changing the security and design concept every five years can be adequate, considering the time forgers need to crack the system. However, and for various reasons, you might want to avoid changing the security concept in its whole, or the looks of the document in 5 years' time. In this case, make sure, your concept is fit for today and for the future and can be updated with new technologies.</p>
--

Table 7 – Checklist: “Intelligent Security Concepts”

Be careful not to view a security concept as a menagerie of security features.

The main purpose of security features is to ensure the protection of the data printed on the document.

Too often these features essentially just secure the substrate and use up a lot of space in the process. Remember, that it is basically not about the document, but about the data and the process. Protect the data from manipulation or subsequent insertion. Because if you do that, in most cases the substrate is protected at the same time.

Also consider that the individual components of the security documents should be secured in order to be able to intercept any breaches in the logistics and issuing chain.

If you take this to heart, you will find more space on the document for the data, and probably be able to work more cost-effectively.

Directly related to the specification of a security concept is the question of detail specification. Are proprietary security

EFFICIENT USE
OF SECURITY
FEATURES

PROPRIETARY
SECURITY
FEATURES

features specified? Are zero-deviation specifications issued that commit different suppliers to basically identical results? Or are only framework specifications and targets to be defined, which are then ultimately to be implemented with a certain degree of freedom?

The challenge in the first case is procurement dependency. If proprietary features are specified, you are bound to this manufacturer for the term of the documents. The binding to a manufacturer can then in turn have the consequence that other solutions from other manufacturers are more likely to be unimplementable. On the other hand, the industry is investing in very innovative and effective technologies. Their commercial interest in refinancing the development investments can be considered legitimate and necessary. However, in the procurement of a system, when a solution is specified, the scope for negotiation is limited, as, *de facto*, the decision has been pre-empted due to exclusivity.

RESOURCES



Resources you might want to consider during designing are:

- ICAO Doc 9303, Part 2: Specifications for the Security of the Design, Manufacture and Issuance of MRTDs (Free download from the ICAO website):
<https://www.icao.int/publications/pages/publication.aspx?docnum=9303>
- EU Council Regulation No 1030/2002, 13. June 2002, laying down a uniform format for residence permits for third-country nationals:
<https://eur-lex.europa.eu/legal-content/en/LSU/?uri=CELEX%3A32002R1030>
- EU Council Regulation No 2252/2004, amended 26.06.2009 on standards for security features and biometrics in passports and travel documents issued by Member States:
<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32004R2252>
- Secure Identity Alliance (SIA) eSAM eSecurity Awareness Model
<https://secureidentityalliance.org/ressources/esam>

45. Harmonized visual data-layouts

Before starting into the actual harmonized visual data-layouts, we need to ask ourselves, what the value of harmonization is. After all, the needs can vary from country to country, as names can be quite long in some cultures, or the requirements for amount of data can depend on additional use-cases.

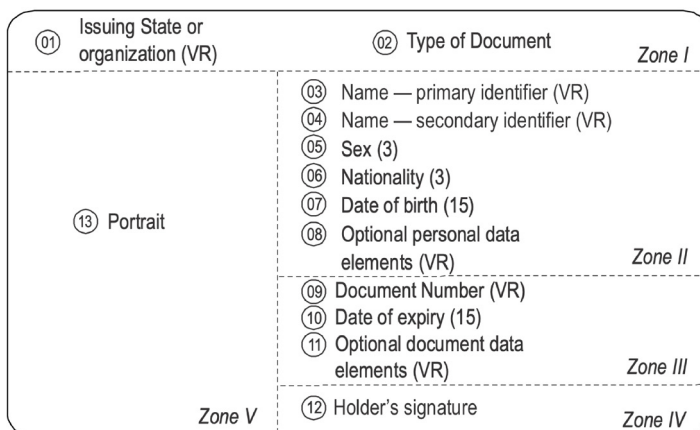
It is perhaps exactly these diverse requirements that stand in conflict with an efficient international interoperability. The harmonization of the visual data-layouts is based on a common denominator, setting rules for important common needs such as data formats and placement.

When setting up a FMZ among countries, you are basically free to use any layout of documents, provided they are not to be used for international air travels outside the FMZ. However, it is advisable to consider the guidance of ICAO set forth in Doc 9303 parts 3, 4 (passports), 5 & 6 (card) and 7 (visa stickers).

It provides a basic structure to the data, so that authorities easily can identify the required data. Also, considerable reflection and field experience go into the guidance on detail aspects such as transliteration, font sizes and other.

The graphic below provides an impression of a generic data structure on the recto and verso of a card.

LAYOUT
ACCORDING TO
ICAO



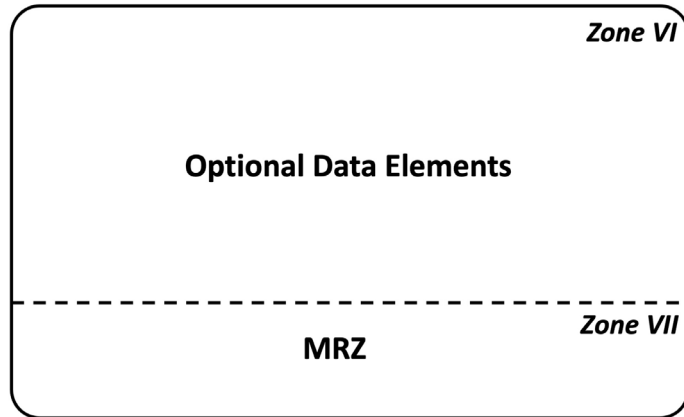


Figure 11 – Zones on recto and verso of an ID-1 format ID-card; ©ICAO Doc 9303

CONSIDERATIONS ON PHOTO SIZE

When computer-assisted biometrics are not used, the portrait is the key element to match a person with a document. Therefore, as a general rule, a larger portrait is a better one. Document 9303 specifies the following for cards, in consideration of all the other data on the document: The portrait shall not be larger than 45.0 mm × 35.0 mm (1.77 in × 1.38 in) nor smaller than 32.0 mm × 26.0 mm (1.26 in × 1.02 in). For passports, the bigger dimension is defined with no variability.

CONSIDERATIONS ON SIGNATURE

The layout defined in above mentioned ICAO Doc 9303 is a compulsory feature. The signature is placed in Zone IV and is rather flexible in its positioning (See Doc 9303-5, Figures 7, 8, 9). The size is regulated: “The displayed signature or usual mark shall be of such dimensions that it is discernible by the human eye (e.g., reduced in size by no more than 50 per cent), and the aspect ratio (A-dimension to B-dimension) of the original signature or usual mark is maintained.”

The value of signatures in authenticating persons might be debatable, and discussions arise every once in a while. However, at this time, the used real-estate cannot be reduced beyond the above definition. An optimization might be considered by providing only small data-capturing fields at time of capturing the original signature. Keep in mind that various actors still rely on physical signatures in their processes, such as banks, contract signing and including public sector.

46. Decisions on access control for eMRTDs

eMRTD chips contain sensitive biometric and biographic information of the holder. The two primary attacks are 'skimming' and 'eavesdropping':

Skimming is the reading of the chip data electronically without the knowledge and consent of the holder.

SKIMMING

If the traveler has his eMRTD in their pocket, and there is no protection against skimming, anybody can read the contents of the chip by holding a reader close to their pocket.

If the communication between the chip and the inspection system is not encrypted, this communication can be eavesdropped within a distance of several meters. This leads to confidentiality issues and tracking.

EAVESDROPPING

To prevent skimming and eavesdropping, two different protocols are defined:

Basic Access Control (BAC) is a mechanism specified to ensure only authorized parties can wirelessly read personal information from eMRTDs.

BAC

BAC requires physical contact with the e-Passport:

- Inspection terminal reads MRZ optically.
- Uses MRZ data to negotiate a session key.
- Chip and inspection terminal generate session key.
- Access to chip data.

Password Authenticated Connection Establishment (PACE) has been adopted to eventually replace BAC.

PACE

While BAC works only with the Machine Readable Zone (MRZ), PACE allows using randomly generated Card Access Numbers (CAN) – short keys printed on the document.

BAC VS PACE ADOPTION



PACE uses asymmetric cryptography, a stronger cryptography than BAC – raising the security of documents to the level of using contact chips.

Be aware: In order to use this method, the eMRTD chip OS must be capable of supporting PACE.

Inspection systems must be capable of reading the chip using either protocol. The majority of the inspection systems use only BAC.

ICAO has set some guidelines which are relevant to Inspection Systems.

- For global interoperability, States **MUST NOT** implement PACE without implementing BAC until 31 December 2017.
- Starting 1st January 2018, States may implement PACE only, without BAC.
- Inspection systems **MUST** support all compliant ePassport configurations. Inspection Systems should implement and use PACE if provided by the ePassport chip.
- BAC will be deprecated in 2025. In this case PACE will become the default access control mechanism.

It is important that inspection systems are able to handle PACE as the access mechanism as this will be the only mechanism used for access control in the very near future.

47. Access control for biometrics

Facial Recognition is considered the primary biometrics for travel and ID documents. It has the advantage that it does not require machine for verification. Comparison between the photo and the person can be done visually by an office without necessarily having to use any technology. To assist in easy access to this biometric for border crossing, it is stored on the chip without any additional access control.

For fingerprint and iris, Doc 9303 recommends additional protection as these are considered sensitive biometric

information. The mechanism to protect them is termed as Extended Access Control (EAC). The mechanism is left to the discretion of the issuing state and is not specified in Doc 9303.

To read sensitive biometric information from the chip, the Inspection System must prove that it is entitled to read the information. A mechanism to enforce such a system is provided for in the definition of LDS2 in doc 9303.

To read more on LDS2 mechanisms see the ICAO Document 9303, part 10: https://www.icao.int/publications/Documents/9303_p10_cons_en.pdf



48. Considerations for biometric capture

An important aspect of harmonising the capture of biometric information is to ensure interoperability across different vendor solutions and national implementations. As a result, it is important to note that the biometrics are stored as high-quality images and not as a template. Below is a list of considerations for biometric capture.

There are some general considerations for biometric images:

- Each input image shall be in 8 bits per colour, e.g., 24 bits per pixel for RGB images (8 bits for Red, 8 bits for Green and 8 bits for Blue), 8 bits per pixel for greyscale images and 32 bits per pixel for CMYK (Cyan-Magenta-Yellow-Black) images;
- The photo image shall be captured on white background;
- The photo image captured shall be stored in both greyscale and colour in 24-bit JPEG2000 format with the compression ratio not exceeding 15:1;
- The photo image shall have a minimum pixel resolution of 420 wide by 525 height; and
- Capture facial, fingerprint and iris images as uncompressed raw images. The images shall be stored in an open standard format such that the Government will not be locked onto a proprietary solution and can change to other facial, fingerprint and iris matching systems without having to conduct an image conversion exercise.

IMAGE CAPTURE

The size and format of the photo image shall comply with the formats indicated in the prevailing ICAO Doc 9303 and ISO/IEC 39794-5. From January 1, 2025, countries may use ISO/IEC 39794-5 to encode the photo image. From January 1, 2030, all images must comply with 39794 and not 19794. Due consideration should be given to this change.

49. Considering special needs

Non-discriminatory systems should be the objective for any issuing authority. Identifying groups of special needs and developing adequate solutions is considered best-practice. When designing documents, special attention should be paid to designing solutions with the visually impaired, the elderly, children, low-income communities and other vulnerable minorities (such as religious minorities) in mind.

VISUALLY IMPAIRED

Use of braille is a renowned approach in designing inclusive documents. Braille is a tactile writing system used by people who are visually impaired. These characters have rectangular blocks called cells that have tiny bumps. The number and arrangement of these dots distinguish one character from another. Braille can be applied both to paper- and plastic-based documents. It can be both individualized or static.

The most important aspect to be decided is what data is to be represented in braille, as the documents have size restrictions. Also, braille can have implications on machine readability.

ELDERLY

Older people may be overwhelmed by technical documents. Education or alternatives should be considered.

CHILDREN

Children change their looks, biometrical data and size quickly. Also, they might not have their own smartphones, which would exclude them to travel, if mobile-IDs were the only option for documentation. With respect to policy, children cannot consent to having their biometric data taken, this need consideration.

50. Where can I find out more about this subject



Documents

ICAO Document 9303, Standards and technical reports
<https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>

ICAO Working Groups: New Technology Working Group (NTWG)

The NTWG develops strategy, policy, specifications and guidance material in relation to the manufacture, security, testing, issuance, deployment and globally interoperable use of MRTDs in both physical and electronic form and global data sharing/exchange for the purpose of holder identification, document validation and secure border control. The Group conducts ongoing research into technology suitable for deployment in MRTDs, issuance and border control environments, and information sharing initiatives and supports the Secretariat in ensuring ICAO Doc 9303 is current and relevant in a changing environment. In addition, it provides support to the ICAO PKD Board.

The Group also provides services such as:

- communications and outreach support to the ICAO Secretariat through a communications sub-group of the NTWG and assists in the development and maintenance of an effective MRTD related communications strategy;
- prepares media-oriented information material on topical issues;
- provides or identifies sources of expert advice to assist the Secretariat in responding to questions from ICAO Member States;
- promotes specifications, standards and ICAO mandates and initiatives;
- develops material and identifying speakers to support organised outreach and educational activity;
- prepares and or identifies material for publication on the ICAO TRIP Platform; and
- assists in the development and maintenance of relationships with organisations that have similar or compatible objectives.

Implementation Capacity Building Working Group (ICBWG)

The ICAO ICBWG was established in 2008 primarily to assist with the universal implementation of Machine-Readable Travel Documents (MRTD), and to build global capability in related identity management disciplines. With the establishment of

the Traveller Identification Programme (TRIP), the mandate of the ICBWG became much broader, incorporating advice and guidance for ICAO Standards and Recommended Practices (SARPs) across a range of travel document and border control/facilitation areas.

States may lack the knowledge, technical expertise or resources to implement ICAO SARPs. ICBWG assists states to comply with SARPs, invest in appropriate systems and technologies, and implement best practice processes to achieve global interoperability and security. The ICBWG key focus is to ensure the ICAO 'No Country Left Behind' mandate is realised.

ICBWG has five enabling outcomes to assist ICAO Member States to uniquely identify individuals and enhance the security, integrity and efficiency of travel document and border clearance operations:

- States effectively establish and authenticate identity;
- States issue travel documents that comply with ICAO Standards and Recommended Practices (SARPs);
- States have robust and secure document issuance systems and controls;
- States routinely read and validate MRTDs (including eMRTDs) at borders;
- States utilise globally interoperable applications to manage risk and maximise border efficiency.

The ICBWG provides advice and assistance to the ICAO Secretariat in the implementation of the five elements of TRIP. This includes (but is not limited to) the following areas of activity:

- Developing guidance material and tools for implementing TRIP-related standards, recommended practices and specifications, and measuring compliance;
- Updating ICAO policy and guidance material on the ICAO TRIP Strategy, with a view to keeping it current and responsive to changes and the needs of ICAO Member States;
- Supporting capacity building initiatives and regional initiatives, including seminars and symposia;

- Facilitating ICAO TRIP assistance in the form of education, training and identification of experts for projects conducted through a resource mobilisation process or voluntary contributions;
- Building the knowledge and strategic capability of States in order that they can design, procure and implement new technologies and processes that drive value;
- Maintaining up-to-date information on the status of States in relation to travel documents and border control; and
- Contributing to the development and maintenance of SARPs and technical specifications on MRTD or eMRTD issuance and border control matters, including serving as a forum for providing input and feedback.
- The ICBWG also undertakes a proactive leadership role for ICAO in facilitating and coordinating assistance in the international community, in close cooperation with other experts of Member States, international organisations and the private sector.
- The ICAO Secretariat, TAG/TRIP members and ICAO Member States can attend ICBWG, TAG/TRIP Observers, Chair of the ISO SC17 WG3, Task Force Leaders and representatives from other interested parties and organisations are invited at the discretion of ICAO or the ICBWG Chairperson.

CHAPTER 9

NON-PHYSICAL CREDENTIALS



What you will learn about in this chapter:

- Forms of non-physical credentials
- Important considerations when contemplating the introduction of non-physical credentials
- Where to find more up-to-date information on this work-in-progress subject

51. What are the forms of non-physical credentials

A developing area of credentials focuses on non-physical credentials, such as the Digital Travel Credentials (DTC) that is being specified by ICAO.

Such initiatives are aimed at seamless travel and border crossing and tend to focus on biometrics as a token, rather than the presentation of a physical form factor like a passport or ID card.

Another initiative is the Mobile Driving Licence (mDL), which is currently being specified (and is being piloted in a number of UN Member States). It allows for a mobile phone (smart phone) to store the driving license and present it to an inspector for verification.

52. Considerations when contemplating the introduction of non-physical credentials

Before looking at the considerations for the introduction of such credentials, it is worthwhile to reflect on the role of physical credentials.

A person's identity is defined by their combined biometric and biographic attributes that apply uniquely to that person. A credential is then issued to the person after their identity has been verified and enrolled.

The credential, in the form of a travel document or an identity card, contains the biographic and biometric information that have been verified. So, the credential acts as a container of this information.

If the biographic and biometric information are stored in a database and then used to verify the identity of the person before allowing them access to their entitlements, is the physical credential still required? What role does the physical credential play?

As mentioned, the biographic and biometric attributes of a person uniquely identify the person. Matching the biometrics binds the identity to the person.

The presentation of the credentials establishes the entitlement of the person to claim that identity. So, the physical credential acts as a second factor to the identity.

Biometric matching always returns a confidence level that the person being identified matches with the presented biometric token. This confidence level is never 100%. A variety of factors like ageing, lighting conditions during the capture of biometrics etc. influence the confidence level.

It is important to remember that any non-physical credential that is issued must always be backed up by a physical credential. This is to cater to cases where the confidence level of the biometric match is low or when lookalike fraud (or the case of identical twins) is suspected. So, there is no pure non-physical credential.

This approach of issuing non-physical credentials backed up by a physical token for a second factor is called a Hybrid Model, and is the model used by the ICAO DTC.

Considerations for non-physical credentials	
<input type="checkbox"/>	<p>Is it backed by a physical credential?</p> <p>A purely non-physical credential will have to rely on the accuracy of the biometric match to tie it to a specific individual. It would be wise to have a physical credential as a backup in case the non-physical credential is not sufficient to establish the identity of the person.</p>

CHECKLIST



<input type="checkbox"/>	<p>Presentation of credential?</p> <p>When a person needs to present their credential for verification, what mechanism would they use? For example, in the case of travel, the information may be sent as part of advance passenger information. If it is not sent as advance information, then the passenger must have some means of handing over the credential to the border control officer. Is this done by using a smart phone, a QR code etc.</p>
<input type="checkbox"/>	<p>Is an online connection needed for verification?</p> <p>Very often, non-physical credentials rest in a database and need to be retrieved for verification of the person. This means that online connectivity would be required from the point of presentation to the backend database.</p>
<input type="checkbox"/>	<p>Interoperability with other states?</p> <p>Non-physical credentials work well within a single economy. If it is to be used across a Free Movement Zone, then mechanisms to be able to verify them must be interoperable.</p>
<input type="checkbox"/>	<p>Cost of securing the infrastructure?</p> <p>If non-physical credentials are stored centrally, then extra care has to be taken to protect it from Cyber threats and compromises. This adds a cost to maintaining this infrastructure and may be higher than the cost of issuing a physical credential.</p>

Table 8 - Checklist: Considerations for non-physical credentials

53. Where can I find out more about what is going on in this field

To read more on non-physical credentials see:



VDS: ICAO Document 9303, part 13:

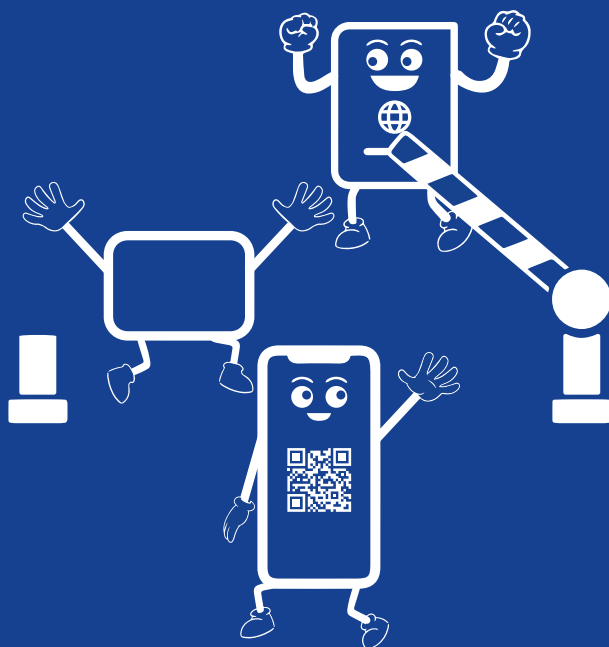
https://www.icao.int/publications/Documents/9303_p13_cons_en.pdf

mDL: ISO/IEC 18013

For sale at your national standardization body. Some parts are still under development

PART IV

DESIGNING AN ADEQUATE BORDER MANAGEMENT





INTRODUCTION TO THIS PART

Part 4 covers Theme C mentioned at the beginning of this guide. It presents the technical aspects of credentials from the perspective of a border control practitioner. The aspects covered here apply to effective border management in general, with specific aspects as they apply to the free movement of people.

This part guides you through relevant aspects in designing an effective border management strategy with a mix of technology, processes and traveller differentiation. After having worked through these chapters you will have a basic understanding of various options, their characteristics and some dependencies.

CHAPTER 10

MANAGING TRAVELLER EXPERIENCES



Any effective border management system design should start by considering the needs of the traveller. This customer centric-approach will enable a border control design that improves facilitation while also improving security.

What you will learn about in this chapter:

A customer centric approach starts off with differentiating between the types of travelers that you will encounter at your border. This was covered in [section 26: “For which user groups”](#). Depending on the type of traveler, different workflows may be adapted. This chapter covers some options for such differentiation.

54. Options for traveller management at the borders

Traveller management depends on the type of traveller and the port of entry. Differentiation in the treatment of traveller groups is necessary for both facilitation and security.

Traveller management can be affected by a technology and/or processes.

The first thing to consider is the structure of the border itself between the members of the FMZ.

There are a few choices that can be made

OPEN BORDERS

Open borders are essentially borders without any immigration or security checks. This is similar to the situation in the Schengen travel area, where there is no border control between Member States.

The only border would be the external border of the FMZ.

CONVENTIONAL BORDERS

While citizens of an FMZ might have free travel within the FMZ, there may still be physical borders. This may be due to the lack of a combined visa policy across the FMZ and to control the movement of non-citizens across the internal borders of an FMZ.

To differentiate and provide preferential treatment for citizens of FMZs, the following options may be considered:

- Separate lines for members of the FMZ;
- Use of automated gates for members of the FMZ.



A user centric approach that offers differentiated treatment of travelers could be derived from some existing travel arrangements. For examples of such existing arrangements, please refer to section 6: “What are the different types of existing travel arrangements”.

CHAPTER 11

DOCUMENT VERIFICATION



What you will learn about in this chapter:

- An introduction to document verification of official travel documents in the context of FMZs
- Additional aspects related to in-official ID documents
- Where to find additional supporting resources

55. Procedures for document verification of official travel documents

A first question that we need to answer is: Why are we verifying the authenticity of official travel documents? And the second question is: Why would someone counterfeit or manipulate such documents? Finding the answer to both questions after thorough reflection, will assist not only in following the recommendations below, but put yourself and your organisation in a position to keep up with ongoing and future developments in this field.

The key questions guiding our assessment are:

- Is the traveller the rightful holder of the travel document being presented?
- Is the document valid and authentic?
- Is the traveller's immigration status defined by their travel document (e.g., citizen of the country, citizen of a regional free travel area, diplomat)?
- Does the traveller qualify for entry or departure according to national or regional immigration legislation?
- Is the traveller admissible at his/her next destination?

The following checklist will provide some guidance on procedures involved. Border control officers should be expert in inspecting and verifying the security features of their own national travel documents, as well as those of other States' travel documents that are commonly encountered on their border. Relevant training to achieve this expertise should be a high priority for border control agencies.

CHECKLIST



Validation of passport documents

Authenticity of document

- Does the document actually exist, or is it a phantasy document?
- Integrity of security features and used technologies?
- Integrity of represented data?
- Consistency of data (visual, digital on document, database)?

- Any signs of unusual wear and tear?
- Binding of passport intact? (e.g. passport number)?

Validity of document

- According to visual and digital data.
- Entries in Interpol SLTD and other DBs.
- According to policies if this document is valid for the use it is being presented.

Matching carrier with document

- Plausibility of data / Interview.
- Facial matching. Make sure that physical and electronic data are consistent (sometimes represented in several technologies on the document). Special attention is required to identify:
 - a. morphing of data (digital recombination of two non-identical pictures);
 - b. Overlaying of additional pictures;
 - c. Manipulation of photo (mechanical/chemical abrasion);
 - d. Impostors. These are people looking similar, but not being the actual rightful holder of the document.
- Biometrical matching of portrait on document, electronically stored data and data in local databases. See chapter 12: “Automated Border Crossings” and chapter 13: “Biometrics for border management” below.

Table 9 – Checklist: Validation of ID documents

Having access to information pools is instrumental to enhancing training and expertise of border control officers. There are three types of data sources what we would like to highlight:

DATA SOURCES

Databases

- Electronic Documentation Information System on Network (EDISON TD):
<http://www.edisontd.net>;
- The EU database of False and Authentic Documents Online (FADO) – which is only available for EU law-enforcement agencies:
https://ec.europa.eu/home-affairs/orphan-pages/glossary/false-and-authentic-documents-online-fado_en

The public version of FADO, the Public Register of Authentic travel and identity documents Online (PRADO):

<https://www.consilium.europa.eu/prado/en/prado-start-page.html>

- INTERPOL has developed the Digital INTERPOL Alert Library-Documents Database (Dial-Doc) to counter the illicit use of fraudulent travel documents and foster international cooperation by exchanging national alerts on recently detected forms of false travel documents through INTERPOL's I-24/71
- Other commercial solutions.

Sample Collections

Digital documentations are convenient as they are readily available in decentralized infrastructure. However, having reference document collections of original and counterfeit documents are important for deeper analysis of questioned documents. Also, they are instrumental for trainings and legal testimonies. The structuring of such collections depends on the national organizations and geography. Many countries have separated the collections of authentic reference documents from the counterfeit collections. This depends on which agency is liaising with the international counterparts potentially via the embassies, and which agencies get to analyse the most questioned documents and gets to testify before court.

Liaison

Finally, a great opportunity within a Free Movement Zone are liaison offices among countries. Within the legal framework they provide direct communication and expertise on questioned documents.

A proven structure of document inspection is organized in three tiers:

- **Front Line (1st level):** Handling of the bulk of documents. If irregularities are suspected, the document (and the traveller) is passed on to the next inspection level.
- **Second Line (2nd level):** Often still on-site, this small

ORGANIZATION

lab can make use of databases and enhanced equipment for inspecting documents. Having this level on-site (e.g. in the airport) allows for regular use without logistical challenges, or facing hindering time-constraints imposed by law.

- **Forensic Lab (3rd level):** Forensic specialists can make use of professional tools, enabling them to inspect third level security features, connect with experts and liaison officers / foreign embassies if required. It is often here where the officers have the capacity to create legally sound reports on the questioned documents.

ICAO TRIP Guide on Border Control Management (BCM)

- Part 1: Guidance:
<https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20TRIP%20Guide%20BCM%20Part%201-Guidance.pdf>
- Part 2: Assessment Tool
<https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20TRIP%20Guide%20BCM%20Part%202%20Assessment%20Tool-FINAL.pdf>

ADDITIONAL RESOURCES



56. How are eMRTD verified

For an overview of the eMRTD Trust model, please refer to annex 1: “Some technological fundamentals”. In this section, we will see how eMRTD Verification (verifying the contents of the chip) works in practice.

Many of the following terms are explained in annex 1: “Some technological fundamentals”, primarily chapter 14: “PKI and the chip in travel documents”.

A few relevant terms:

DSC = Document Signer Certificate

CSCA = Country Signer Certificate Authority

CRL = Certificate Revocation List

SOD = Security Data Object



The data in the chip is organised as Data Groups. To ensure the integrity of each of the Data Groups, the following process is undertaken:

- A Hash is created of each of the Data Groups;
- The hashes are then put into a file called Security Data Object (SOD);
- The SOD is then signed using a Document Signer Certificate (DSC), and the DSC is included in the SOD;
- The SOD is then stored on the chip as a file called EFSOD.

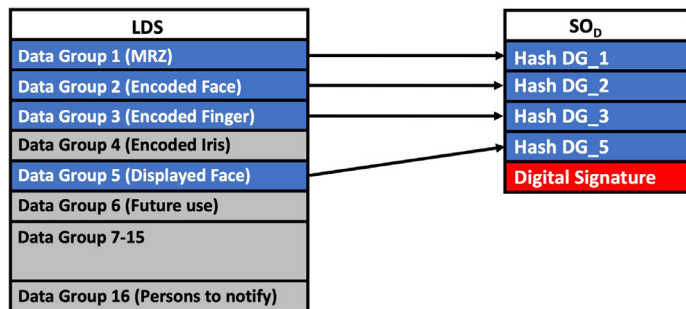


Figure 13 - Structure of the Logical Data Structure and the Security Data Objects | ©ICAO

When verifying the passport, the following process is carried out:

- The Data Groups are read from the chip and EFSOD are read from the chip;
- The signature on the SOD is verified using the DSC contained in the SOD;
- The DSC is then verified against the CSCA of the country;
- The CRL of the country is checked to ensure that the DSC is not known to be compromised;
- Each of the Data Group is then hashed and the hashes are compared with the hashes stored in the SOD;
- If all the above steps succeed, then it is assured that the contents of the chip have not been tampered with and can be trusted.

57. Preconditions for successful eMRTD verification

PRE-REQUISITES FOR eMRTD VERIFICATION

As can be seen from the above steps, to ensure that we can fully verify the contents of the chip, we need the CSCA of the issuing country and the CRL of the country.

So, how do we get the CSCA and the CRLs?

The standard mechanism for exchange of CSCA is diplomatic exchange. Remember that CSCAs are self-signed certificates, so they cannot be verified against any other certificate. So, the exchange of the CSCAs has to happen by means of an agreed process whereby the receiving country can ensure that they have received the CSCA from the passport issuing authority of the issuing country. CSCAs are generated every 3 to 5 years, so once a proper handover has happened, you can verify that countries' eMRTDs without needing any other exchange with the country.

CRLs are another important requirement to complete the verification. CRLs are usually issued every 90 days and more frequently in case there has been a compromise of any DSCs. The CRLs can be distributed by two means:

- Through diplomatic exchange similar to the CSCA;
- Publishing to a website belonging to the issuing country.

Since the CRL is signed by the CSCA of the country, receiving countries can download the CRLs from the website and verify the CRL before using them.

But, if you had to do this with each country that issues an ePassport, imagine the number of diplomatic exchanges that are required and the number of websites to download the CRL from.

To simplify the exchange of the credentials (CSCAs, DSCs, CRLs) that are required to verify an eMRTD, ICAO has established the PKD.

ICAO PUBLIC KEY DIRECTORY (PKD)

eMRTD issuing countries become PKD members and can then upload their DSCs and CRLs to the PKD and similarly, they can download the DSCs and CRLs of the other PKD members. This simplifies the exchange of credentials between the member countries.

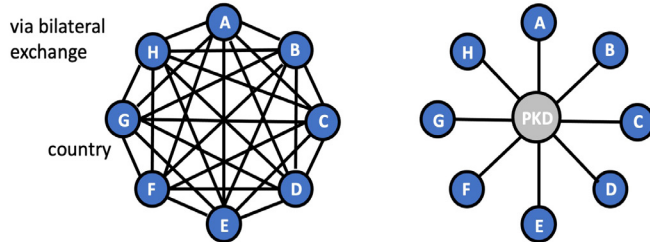


Figure 14 – Visualization of the complexity of having only bilateral DSC and CRL exchanges versus using the PKD for distribution. | ©ICAO

The PKD does not publish the CSCAs of the countries. However, there is another mechanism through which CSCAs can be obtained.

CSCA MASTER LIST

A Master List is a digitally signed list of CSCAs that are trusted by the receiving state.

To understand the Master List, let us take the following scenario:

1. Assume there are 4 countries A, B, C and D.
2. Let us say that a diplomatic exchange has been done between Country A and Country B, and they both have each other's CSCAs.
3. Also, country C and D have also done a diplomatic exchange with country B.
4. So, country B has the CSCAs of A, C and D, while each of them has the CSCA of B.
5. B now issues a Master List containing the CSCAs of A, C and D and also includes its own CSCA in the list. This list is then signed by country B and published on a website.
6. A, C and D then download this Master List and can verify it using the CSCA of country B. If they have confidence in the processes that B has followed in

obtaining the CSCAs, they could trust the CSCAs of the other countries. So, A, C and D have the CSCAs of each other without having done a diplomatic exchange.

In this way, based on the trust in the processes followed by an individual country, CSCA exchange is simplified.

Many countries publish their Master Lists to the ICAO PKD. Similarly, ICAO itself published a Master List containing the CSCAs of all PKD member countries. By downloading the Master Lists from the ICAO PKD, countries can obtain the CSCAs that are required at the border to verify eMRTDs.

Without the CSCA of the country no reliable verification of the eMRTD can take place.

As is obvious, countries must distribute their CSCA to other countries to enable verification of their passports overseas and becoming an ICAO PKD member and uploading their credentials to the ICAO PKD helps with this distribution. Similarly, they must download the contents of the PKD and distribute them to the border control inspection systems.

More information on ICAO PKD can be found here:
<https://www.icao.int/Security/FAL/PKD/Pages/default.aspx>



OTHER
PRECONDITIONS



58. Does ePassport verification always give a yes/no answer

Does ePassport verification always give a Yes/No answer? The short answer is NO.

Most Inspection Systems use a traffic light system to indicate the results of the eMRTD verification.

- Green → eMRTD verification succeeded.
- Amber → eMRTD verification could not be completed.
- Red → eMRTD verification failed.

If the result is a Green, then the course of action is quite clear. The document has been verified and can be trusted. That is, provided the evaluation criteria has been defined and implemented correctly.



TRAFFIC LIGHT
PROBLEM

AMBER

What if it shows Amber?

The conditions under which an Amber is shown depends on the design of the Inspection System and cannot be covered in detail for each type of Inspection System.

For example, if the CSCA of the country is not available to the Inspection System, it may display an Amber result. There are two possibilities for this scenario.

One, a diplomatic exchange has not been done with that country and the CSCA is not available from any Master List. In this case, the document may be a valid document but the Inspection system does not have the credentials required to finish the process.

However, there is a second possibility. The eMRTD is a fake document that has been personalised with a phantom CSCA. In this case, it is a fraudulent document.

An automated process cannot make the determination which of the above two scenarios apply when an Amber condition is reached, and this will require manual processing.

RED

Does a Red definitely mean a fraudulent document?

Unfortunately, the answer is NO.

eMRTDs have to be issued in compliance with the requirements of Doc 9303. It is a fact that many countries have made some errors in the encoding of the chip data, due to which, eMRTD verifications can fail even for valid documents. Again, a manual processing is required to ascertain whether this is defective but valid document or it is a fraudulent document.

Defect handling should be implemented in Inspection Systems, but unfortunately, very few systems actually do that. This results in a significant number of false negatives, where valid documents are flagged as being fraudulent.

The problem with Amber and Red is more pronounced in automated processing.

We will be providing some more information on this subject in chapter 12: “Automated Border Crossings”, especially section 65: “What if something goes wrong, and how can we know”.

59. How to manage Automated Border Crossing

In the previous section, we covered the validation of the eMRTD. However, this only proves the authenticity of the travel document. The binding to the person presenting the document has to be done to establish the authenticity of the traveller.

The binding between an authenticated travel document and the traveller is done by matching the image of the person presenting the document to the facial image stored in Data Group 2 of the chip of the ePassport. For other biometrics considerations see section 68: “What to consider when using biometrics on the borders”.

This matching may be done either visually (the DG2 image is displayed to the officer and he visually compares the image to the person standing in front of her) or by using automated facial recognition (using a camera to capture image of person presenting the document and comparing it to the DG2 image).

For travellers that from an identity management perspective are deemed low-risk (e.g., citizens, residents, travellers from specific countries), there is no need for a border control officer to interact with the traveller. In such cases, the process of authenticating the travel document and doing the biometric binding to the traveller can be done using machine authentication without the involvement of a dedicated border control officer. Such a system is known as Automated Border Crossings.

60. Guidance for document verification of non-passport documents

Verification of non-standardized documents are a major challenge. In the best case, your agency has its own database and sample catalogue of documents that have positively been identified as authentic or counterfeit. Or you have access to databases provided by the issuing country.

BINDING TO THE
TRAVELLER

However, this is rarely the case in a comprehensive manner, including birth certificates or other vital records, diplomas, student or military ID, member of special status citizens documentation etc.

So, as a first step, it is important to make sure your regulation provides clear grounds as to what kind of documents serve which rights. Other documents might then serve for validation.

Important tools are the training of staff in interview and inspection techniques, use of appropriate validation tools such as UV-Lamps and magnifiers, databases and sample collections, as well as a well-functioning secondary inspection unit and liaison offices with the Member States. Furthermore, an important training method is to teach inspectors how to validate the most commonly used security features and techniques, watermarks, DOVIDs, guilloche, intaglio, latent image, etc. Whilst they may not know the watermark of a passport of any given country they will then be able to say that it is in fact a real or fake watermark.

CHECKLIST



Validation of non-passport documents	
Data-Check	
<input type="checkbox"/>	Is the data plausible? E.g. data of issuance with age of person or version of document; occupation and travel plan etc.
<input type="checkbox"/>	Is the data consistent across all presented documents?
<input type="checkbox"/>	Is the data verifiable with reliable online-resources / databases?
<input type="checkbox"/>	Check for spelling errors in the form and in the personal data that do not appear to be explainable as errors by the issuing body.
<input type="checkbox"/>	Interview: Does the data mentioned and story match the documents?
Authenticity	
<input type="checkbox"/>	If database or collection available: Do the documents match the documentation in respect of substrate, print, data-entry technology, formatting. If information available, make sure that the findings match regional differences or changes in specifications in time.

<input type="checkbox"/>	If in doubt, check with embassy or liaison office if the document type actually exists, in order to avoid accepting professional looking phantasy documents.
<input type="checkbox"/>	Are the documents preprinted in conventional printing technologies, rather than office/home printers?
<input type="checkbox"/>	Is the substrate UV-dull / non-fluorescent?
<input type="checkbox"/>	Are any signs of chemical or mechanical abrasion / modifications apparent?
<input type="checkbox"/>	Any signs for unusual wear-and-tear that might serve to hide manipulations or irregularities?
<input type="checkbox"/>	Check authenticity of stamps, seals.
<input type="checkbox"/>	Check security features present for their authenticity.
<input type="checkbox"/>	Are the technologies applied to the document consistent with the issuing date? This applies especially to birth certificates Fun-fact: First commercial inkjet printer available from 1984; First commercial laser printer available from 1984. However, both at price points that make it unlikely that they were used in civil registration offices at that time already.)

Table 10 – Checklist: Validation of non-passport documents

61. Where can I get additional information on the subject

A more detailed guide is provided in the [ICAO TRIP Guide on Border Control Management](#). The [ICAO Traveller Identification Programme Guide on Border Control Management](#) is intended for reference by States to optimize the use of the tools, systems and applications available to enhance their national BCM. The Guide includes 13 technical topics describing and categorizing the Inspection Systems and Tools and Interoperable Applications that can be applied for this purpose



ICAO TRIP Guide on Border Control Management

Part 1: Guidance

<https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20TRIP%20Guide%20BCM%20Part%201-Guidance.pdf>

**ICAO TRIP Guide on Border Control Management
Part 2: Assessment Tool**

<https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20TRIP%20Guide%20BCM%20Part%202%20Assessment%20Tool-FINAL.pdf>

Guidance on inspecting documents:

[IOM, 2016, 'PEPM II - Passport Examination Procedure Manual', Geneva](#)

IOM, 2017, 'Document Examination Laboratory Manual for the Immigration Environment', Geneva

CHAPTER 12

AUTOMATED BORDER CROSSINGS



What you will learn about in this chapter:

- Mechanisms to deploy automated border crossings
- What they can and cannot do
- Handling exceptions
- Handling document defects

62. What are Primary Inspection Kiosk machines (PIK)

Foreign travellers have to submit a form of declaration when they enter a country. These are termed as Arrival Cards or Disembarkation cards and usually involve declaring a few things:

- Full name;
- Travel document number;
- Place of residence;
- Flight/Vessel/Vehicle number on which the traveller arrived at border;
- Address in destination country;
- Contact details;
- Port of embarkation;
- Health declarations;
- Customs declarations – dutiable goods;
- Financial declarations – Amount of cash or foreign currency;
- Travel history;

The mechanism to submit such information is usually in the form of a card that needs to be filled out and submitted to the border control officer. The officer then checks the information and may enter it into the border control system, or such data entry may be done later. This data is used for risk assessment and admissibility of the traveller.

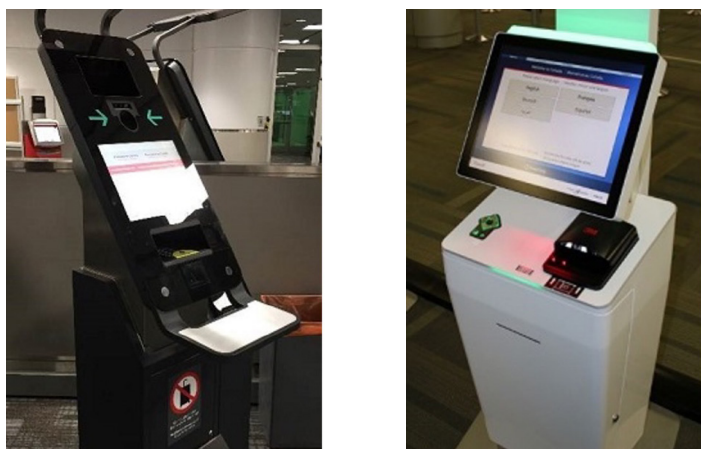


Figure 15 – Samples of PIKs | © CBSA-ASFC | <https://www.cbsa-asfc.gc.ca/travel-voyage/pik-bip-eng.html>

Primary Inspection Kiosks (PIKs) are a means to automate this process and allow the traveller to enter this information. It has a few advantages:

Since the traveller enters the data at a Kiosk, this information can be recorded automatically. This eliminates the data entry by the border control officer or by a back-end process. The information can be fed directly into the border control system.

A rule-based engine can be deployed to ask additional questions based on the information that is entered by the traveller. This allows for more extensive data capture for cases that need further information. An artificial intelligence (AI)-based system would also be able to use that information for pre-screening before the travellers meets a border control officer.

One of the most time-consuming elements of border crossings is the capture of biometrics of the traveller. This activity can be done at the PIK thus relieving the border control officer from this task.

Arrival/Disembarkation cards need to be re-printed if additional information is required. For example, in case of a pandemic, the health-related questions may be added. In a PIK environment, re-configuring the terminals to ask the questions can be very easy, fast and economical

A possible alternative to a PIK is a mobile app that the traveller can download and use to submit their declaration.

CBSA website

<https://www.cbsa-asfc.gc.ca/travel-voyage/pik-bip-eng.html>

SELF-ENTRY BY
TRAVELLER

RISK
ASSESSMENT
CAPABILITIES

BIOMETRICS
CAPTURE

DYNAMIC FORM
GENERATION



63. What are eGates

E-Passport Gates (eGates), sometimes referred to as Automated Border Control (ABC) Gates, are automated self-service barriers that can be used by the traveller to cross the border as an alternative to being processed by an officer manually.

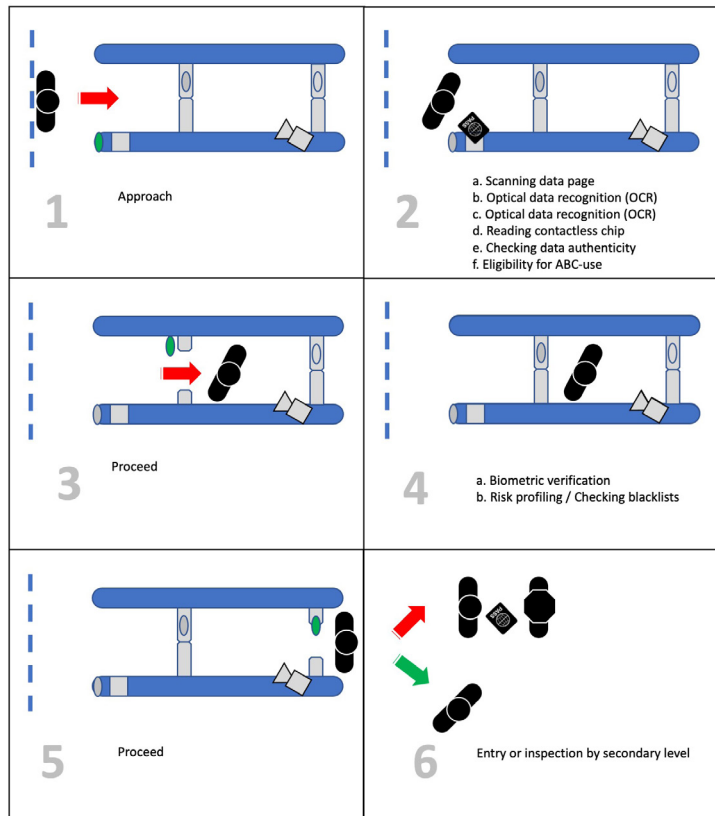


Figure 16 - User-experience and process steps during the operation of an eGate

eGates can perform a variety of functions

MACHINE ASSISTED AUTHENTICATION OF SECURITY FEATURES

eGates have the capability to capture an image of the travel document and compare it to a database of exemplars on record. This comparison enables the detection of fraudulent documents based on the physical security features of the travel document

READ INFORMATION FROM CHIP

The eGates scan the Machine Readable Zone (MRZ) of the travel document and use the information to establish a secure communication to the chip and read the contents of the chip

VERIFY THE AUTHENTICITY OF THE INFORMATION ON THE CHIP

The data in the chip is protected using Public Key Cryptography (PKC) and is digitally signed by the issuing country. The eGate is capable of establishing the authenticity of the information on the chip by verifying the digital signature. Any attempts at tampering of the data can be detected with accuracy.

Without the CSCA of the country no reliable verification of the eMRTD can take place.

The eGate can use Active Authentication (AA) or Chip Authentication (CA) to detect any cloned travel documents.

The eGate uses the image of the traveller read from the chip for Facial Recognition (FR) to verify the traveller's identity.

The eGate uses the biographic and biometric information obtained from the chip to query watchlists and other databases.

The facial image of the traveller can be read using secure messaging. Sensitive biometrics like fingerprint and iris are usually protected using extended access control. eGates can read these biometrics and allow for multi-modal biometric verification. Multi-modal biometrics refers to verifying different biometric markers. For example, both the face and the fingerprints are matched.



CLONE DETECTION

BIOMETRIC
MATCHING

LOOKUPS

EXTENDED
BIOMETRICS

64. What can eGates do

eGates carry out the automated verification of the travel document and also verify the identity of the holder. They also do automated lookups on watchlists and databases and can decide on eligibility of the traveller to enter the country.

A word of caution: The result of the FR to the traveller is a confidence score. If the score is above the threshold, then it is considered as a pass, or else it is considered a "Fail". The confidence threshold has to be set in a judicious manner. If too high, there will be many false rejects and a low value will lead to allowing imposters and lookalikes to enter on invalid travel documents.



When all functions pass, the result is a pass decision. When any check fails, there needs to be a process of exception handling.

65. What if something goes wrong, and how can we know

Exception handling is required for any of the following reasons.

- The passport could not be read.
- The biometric match is below the threshold value.
- The verification of the passport failed or did not succeed.
- A clone passport was detected.
- There was a 'hit' on a terror/criminal watchlist.

Typical deployment scenarios for eGates are as follows.

A set of eGates are connected to a command centre, where the results are displayed on a monitor and an officer is responsible for monitoring the results of the traveller.

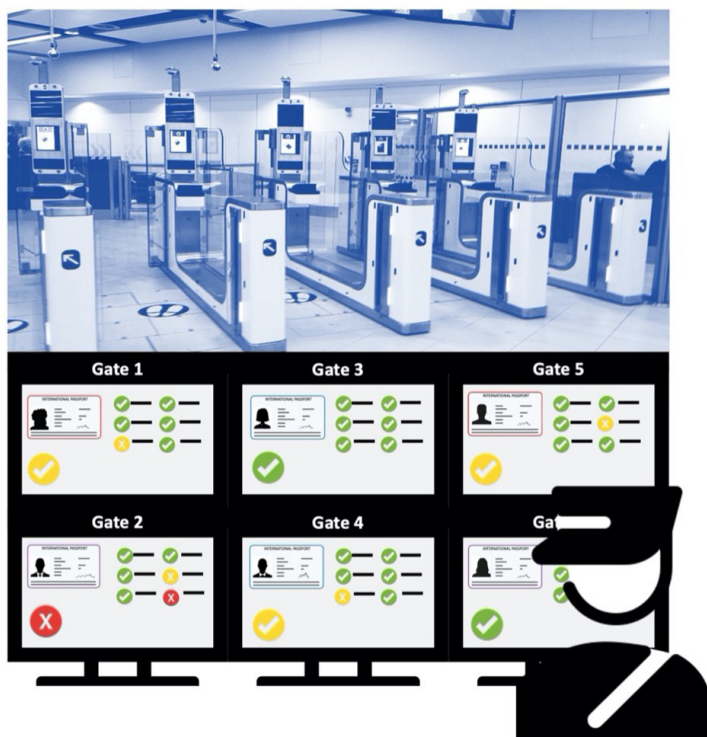


Figure 17 – ABC-gate monitoring in command centre © Figure by authors.
Photo of ABC-gate: Elliott Killingbeck https://commons.wikimedia.org/wiki/File:GAT_South_eGates.JPG

In case of a failure, an alarm is displayed to the officer. The officer then needs to take a decision on whether to allow the traveller to enter the country or send them to secondary processing

There are a number of reasons for which failure may occur. Depending on the type of failure, the result could be a Red or an Amber. The following is a non-exhaustive list of errors and what should be done in response.

RED / AMBER / GREEN LIGHT PROBLEM

- **MRZ read error** – If there is a read error on the MRZ, then the chip cannot be accessed. This error may be shown as a chip read error. Verification of the document, verification of the identity of the holder and the anti-clone detection will all fail as they are dependent on the reading of the chip. The traveller should then be sent to manual processing.
- **Chip read error** – A chip read error may happen because of faulty chip or an intentional damage to the chip. Fraudsters that wish to manipulate the Visual Inspection Zone of the passport will try to damage the chip to bypass PKI verification. Any chip read errors must be referred to manual processing.
- **Biometric matching error** – If the confidence level is below the threshold, then biometric matching will fail. Low confidence levels for biometric can arise from a variety of natural factors like ageing etc. but could also be an indication of imposter or lookalike fraud. The traveller should be referred to manual processing.
- **ePassport verification error** – The PKI verification of the ePassport fails. This could be a case of actual fraud. However, there are also cases of defects in passports that cause such failures. Any such failure should be processed at Secondary. However, if a large number of failures occur, and are later deemed to be valid travel documents, then an analysis of the failure cases and improvement in the defect management capability of the eGate has to be undertaken.

- **ePassport verification not completed** – If the CSCA of the issuing country is not available to the eGate, the process of ePassport verification cannot be completed. However, it could also be a case of fraud using phantom CSCAs. The traveller should be referred to secondary processing. Effective update policies to ensure that all CSCAs are available at the eGate must also be enforced.
- **Physical Security verification failed** – Provided the eGates are capable of validating the physical security features presented, this should be considered. These could be spectral characteristics not matching the specifications, visual data (including photograph) not matching the electronically stored data, or elements missing. Errors can occur based on document wear-and-tear, or actual criminally motivated manipulations.
- **Inconsistent historic data** – The authorities might have been storing identifying data on the travellers in the past and are monitoring irregular changes to the past.

66. What are the prerequisites for proper use of ABC-Terminals

To implement an effective Automated Border Crossing, the following considerations apply:

CLASSIFICATION OF TRAVELLERS

A proper evaluation of travellers that can be considered low risk and hence are allowed to use ABCs is a policy decision. These could be citizens, residents, travellers holding specific passport etc. This classification of travellers is a necessary first step before implementing ABCs.

OBTAINING eMRTD CREDENTIALS

A necessary step of ABCs is the verification of the contents of the chip. This requires that the CSCAs and CRLs of the countries that can use the ABCs are available to do the verification. These CSCAs and CRLs may be acquired from the ICAO PKD or through bilateral exchanges with other countries.



It is important that CSCAs and CRLs are always up to date. CSCAs are issued every 3 to 5 years and CRLs are issued at

least every three months. If these are not updated, verification of new ePassports will fail.

Travellers need to be given proper instructions in the use of ABC terminals. To cater to the widest group of travellers with different language skills, it would be better if the steps to use the ABC are displayed as easy-to-understand pictograms.

Most automated gates do not have the capability to check a visa that may have been issued as a Visa sticker. In this case, it limits the number of nationalities that may be able to use the ABC terminals. A possible solution is to integrate the ABC terminals to a Visa Information System which can be looked up based on the passport number that is read from the MRZ.

In times of a health crises, if the presentation of a Proof of Vaccination or Proof of Testing is required, then the automated gates should be able to process the presented proof of vaccination or the proof of test. If this checking has to be done manually, then the utility of automated gates is marginal.

PROPER
SIGNAGE

VISA CHECKING

HEALTH
DECLARATIONS



CHAPTER 13

BIOMETRICS FOR BORDER MANAGEMENT



What you will learn about in this chapter:

- A summary of considerations when using biometrics at the border

67. What is the role of biometrics in border management

For automated border control, facial recognition is the most widely used biometric.

The facial image of the person is captured using a camera and then compared to the image stored in Data Group 2 of the eMRTD.

The use of fingerprint and iris is usually limited to national documents, due to the sensitivity of allowing other states to read these information from the chip of the eMRTD.

68. What to consider when using biometrics on the borders

There are many ways that a biometric identification system can be deployed.

PRESENTATION ATTACK DETECTION

One of the key considerations is detecting presentation attacks.

A person may present a printed photo, an image on a screen or present a 3D mask to the biometric capture device. This is also known as biometric spoofing.



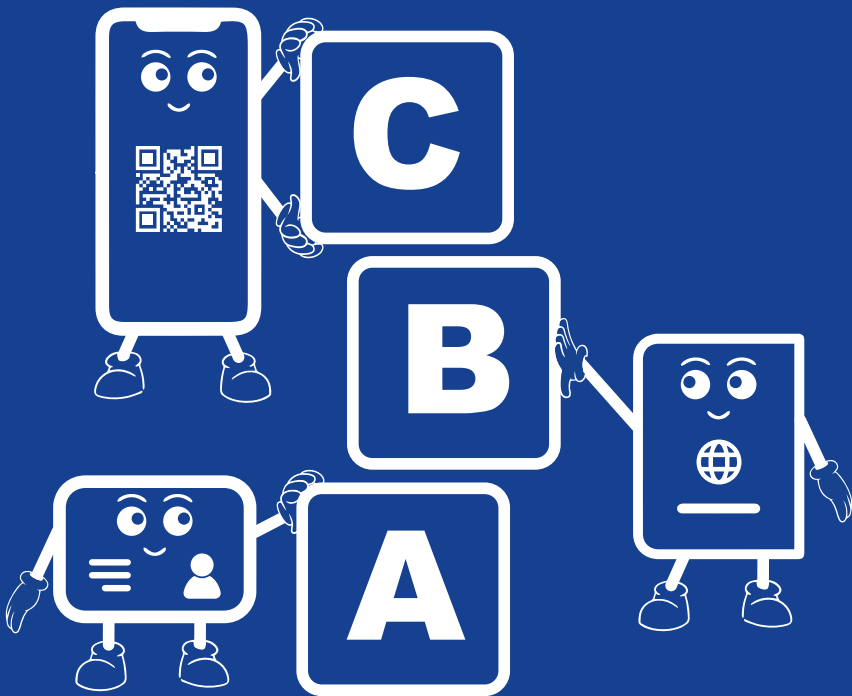
A good document explaining the considerations for presentation attack detection is available from the biometrics institute at: <https://www.biometricsinstitute.org/wp-content/uploads/1809-liveness-questions-final.pdf>

MULTI MODAL BIOMETRICS

Depending on a single biometric feature is not fail-proof. It would make sense to use multiple biometrics like face, finger and iris for verification of the travellers. A key consideration would be the retrieval of the anchor image against which to compare the presented traveller. In case of face, the image is available from the eMRTD. However, the sensitive biometrics like fingerprint and iris, may be protected using Extended Access Control (EAC). In this case, it would be necessary to ensure that the capability to read these biometrics is available in the inspection systems. Some more information on biometrics is supplied in chapter 15 “Biometrics”.

ANNEX 1

SOME TECHNOLOGICAL FUNDAMENTALS





INTRODUCTION TO THIS PART

This annex guides you through some technological fundamentals that underpin travel and identity credentials. It is necessary to understand a couple of foundational technologies that underpin modern identity systems. Since these are mentioned in different parts of the documents, it is essential to have a quick overview on these technologies. This is not an exhaustive lesson on any of the technologies, but is intended to give the reader a basic understanding that should be useful when discussing the usage of these technologies.

“Any sufficiently advanced technology is indistinguishable from magic.”

– Arthur C. Clarke, *Profiles of the Future: An Inquiry Into the Limits of the Possible*

CHAPTER 14

PKI AND THE CHIP IN TRAVEL DOCUMENTS



This chapter provides a short introduction to Public Key Infrastructure that is used to protect the contents of the chip and to ensure that it is tamper evident.

What you will learn about in this chapter:

- A few basic principles of cryptography. This will be useful in understanding the verification process
- Understand the basics of Public Key Infrastructure
- Understand how data is stored in the chip of travel and ID documents

69. What are some core concepts of cryptography

“ One must acknowledge with cryptography no amount of violence will ever solve a math problem. ”

- Jacob Appelbaum, *Cyberpunks: Freedom and the Future of the Internet*

Cryptography is based on mathematical processes. It depends on problems that are difficult to solve. In this section, we cover some basic concepts of cryptography.

HASHING

Hashing refers to a mathematical process that is used to transform data into a form called the message digest or a 'hash'. It has some interesting properties.

Fixed output size:

When you hash a message, the output is always the same length, irrespective of the size of the input message. The size of the output depends on the algorithm used for the hashing function.

The following examples in figure 18 illustrate the point: Hashing the message “A” gives us an output of a size of 20 characters.

You will notice that though the input of message “B” is larger, the output is still the same size.

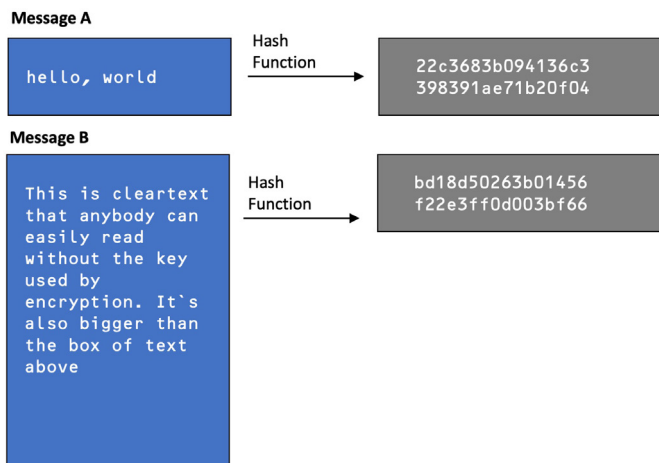


Figure 18 – The input length of the message has no effect on the resulting hash

One Way Function

It is immediately apparent from the examples given above, that once a message is hashed, it cannot be reconstructed from the output. This makes it a one-way function. So, you cannot predict the input from the given output. Additionally, hashing will always produce the same output for the same input, providing the same hashing function is used.

Avalanche effect

A small change in the input message results in a hash value that is dramatically different from the previous hash.

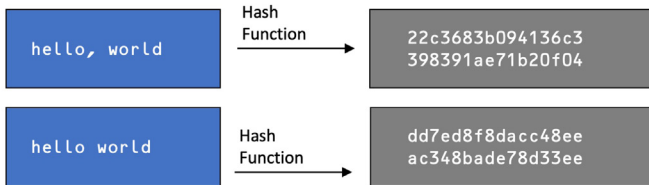


Figure 19 – Avalanche effect of hashing message with minimal deviations

As can be seen in the above example, a small change in the input (a missing comma) drastically changed the output message. This avalanche effect makes it easy to detect the smallest of changes to the input message.

Assume that you are sending a message to someone, who wants to ensure that the message they receive is the same message that you sent and that it was not tampered during the transit. You then send the message along with the hash of the message that you compute. The receiver then hashes the received message and compares the computed hash to the hash that was received with the message. If they match, then the received message is identical to the sent message. If the message has been tampered during transit, the hash that the receiver computes will not match the hash that is sent by the sender. This provides an easy mechanism to protect the integrity of transmitted messages.

However, there is a catch. A fraudster who intercepts the message can modify the message, compute a new hash and send it along with the message instead of the original hash.

WHY IS HASHING
USEFUL

between two parties, an exchange of the encryption keys can be done and then subsequent messages can all be protected using the secret key. However, if you need to exchange such messages with multiple parties at random, such an encryption is difficult to maintain.

This problem is solved by Asymmetric Cryptography, also known as Public Key Cryptography.

In asymmetric encryption, the keys used for encryption and decryption are different. The keys have a mathematical relationship with each other and form a key-pair.

ASYMMETRIC ENCRYPTION

Assume you have a key pair A and B. If you encrypt a message with A and again decrypt it with A, it will not give you the original message. The only way to retrieve the original message is to decrypt using B. This property holds in the other direction as well. If you encrypt with B, the only way to retrieve the original message is to decrypt with A. Furthermore, no other key can decrypt the message encrypted with either A or B.

This opens up an interesting possibility. Assume that you generate a key pair A and B. You then hand out your key A publicly, say by publishing on a web site and you keep B as private. This can then be used as follows:

- Anyone who wishes to send you an encrypted message can then use A to encrypt the message and send to you. Since this message can only be decrypted with B and you are the holder of B, no one apart from you can decrypt the message. This ensures message confidentiality. This solves the problem that we had with symmetric encryption where people had to exchange keys. There is no 'key exchange' that is required and you publish your encryption key (A) publicly. That is why it is also known as Public Key Cryptography.
- Another use case opens up with this setup. If you encrypt a message with B, then anyone who downloads your Public Key can decrypt the message that you encrypted with your Private Key. Since, only you could have encrypted the message with your Private Key, they can be assured that if they can decrypt your message

using your Public Key, then the message has to come from you. This ensures the confidence that you are the originator of the message. The process of encrypting with your Private Key to ensure authenticity of the origin of the message and ensures message authenticity.

So, in a nutshell:

- For message confidentiality, I encrypt with the 'Receiver's Public Key'. The receiver then decrypts with 'Receiver's Private Key'.
- For message authenticity, I encrypt with 'Sender's Private Key'. The receiver then decrypts with 'Sender's Public Key'.

Examples of algorithms uses for Public Key Cryptography are RSA and ECDSA.

The addition of PKC helps solve the problem of message interception we mentioned earlier.

70. Applying the concepts to protect a message

MESSAGE PROTECTION

In the section on hashing, we raised the issue that if a person can intercept the message, they could create a new hash and send it to the recipient. By adding Public Key Cryptography (PKC), we can solve the problem.

This is how it will work on the sender side:

- Hash your message and create the message digest.
- Encrypt the message digest with your Private Key.
- Send the message and the encrypted message digest to the recipient.

On the recipient side, they will follow the steps:

- Decrypt the encrypted message digest using the senders Public Key.
- Hash the received message.
- Compare the two hashes to ensure that they match. If they match, then message has not been tampered.
- If the decryption of the message digest fails, then the

encrypted hash has been modified and cannot be trusted.

- If the decryption succeeds, but the hashes do not match, then the message has been tampered with.

This mechanism is generally called the process of Digital Signature.

So, what is the difference between Public Key Cryptography and Public Key Infrastructure?

In the previous section, we noted that if you wish to ensure the authenticity of the message, we can use asymmetric cryptography and hashing.

PUBLIC KEY
INFRASTRUCTURE
(PKI)

However, a few considerations apply:

- We could, in theory, create a key pair and use that for all messages that need to be protected. However, what happens if the Private Key that we use for these messages gets compromised, e.g., if a third party gets access to your Private Key. In this case, they can digitally sign messages pretending to be you (called spoofing). In this scenario, we would have to create a new key pair and ensure that every one of our intended recipients know that the old keys cannot be trusted and that they should trust the new keys. This would be an operational nightmare if there are a large number of recipients that we deal with, which is typically the case for ePassports, where all the countries that accept your ePassport are recipients. We need a more efficient mechanism for communicating compromise and also for distributing a new set of keys.
- If a Private Key is used to sign a large number of messages, it is theoretically possible to guess the Private Key from the messages. Hence, signing keys must be changed on a regular basis. When the keys are changed, the aforementioned issue of distribution of the Public Key again becomes an issue.

At this point, it is relevant to understand the concept of a Digital Certificate

DIGITAL CERTIFICATE

The Public Key that we created earlier, is just that: a key. However, it does not have any information as to who is the owner of the key.

A Digital Certificate is a digitally-signed structure that is used to convey additional information about the key, which binds the Public Key with an entity and is defined by ITU Telecommunication Standardization Sector.



Figure 23 - Visualization of a Digital Certificate

The above is a simplified representation of the Digital Certificate and there is more information available inside a Digital Certificate. The contents of the Digital Certificate are called fields and each field has a specific purpose.



SOME IMPORTANT FIELDS IN A DIGITAL CERTIFICATE

More details on the definition of the fields used in a Digital Certificate can be found at:

<https://www.itu.int/rec/T-REC-X.509-201910-l/en>

We focus on a few of these fields as relevant to the discussion at hand. The Digital Certificate contains:

- **A subject name** – This binds the Public Key to an entity, which may be a person or an organization.
- **Public Key** – The Public Key that we are trying to distribute.
- **Validity** – We can set the validity of the Public Key, with a start date and an end date. Any signature done with

the corresponding Private Key is only valid within this period.

- **Signature** – To ensure that the information in the certificate cannot be modified, we digitally sign the contents. This begs the question, who signs the certificate. If it is signed using the Private Key, corresponding to the Public Key in the certificate, it is called a **self-signed certificate**. It may also be signed by a different Private Key. The reasons for signing with a different Private Key will become apparent soon.
- **Issuer** – The issuer is the entity that signed the certificate. If the certificate is self-signed, then the issuer is the same as the subject. However, if it has been signed by a different Private Key, then the subject name of the entity whose Private Key was used to sign the certificate is mentioned in the Issuer field.

With this information, we are ready to discuss the two-tier trust model

In the two-tier trust model, we first generate a key pair and get a Public Key and a Private Key. We then create a Digital Certificate that contains this Public Key and sign it using the Private Key. This is a self-signed Certificate.

TWO-TIER TRUST MODEL

We then generate another key pair and create a certificate using the new Public Key, but sign it using the Private Key that we generated previously.

Hence, we now have two Certificates:

- A self-signed Certificate containing the first Public Key.
- A second Certificate containing the second Public Key, but signed by the first Private Key.

In this trust model, we then distribute the self-signed certificate to recipients. We then use the second Private Key to digitally sign the message that we want to protect. When sending the message, we send the second certificate as well along with the message.

So, let us see what happens on the recipient side:

- The recipient takes the message and hashes it;
- They then decrypt the signature using the second Public Key (sent in the certificate that is accompanying the message) and verify the hash;
- Then, they verify the certificate using the self-signed certificate that was previously distributed. If this verification succeeds, then the message can be trusted.

At first glance, this can seem a bit complicated. In reality, the two-layer trust model greatly simplifies the problem of Public Key distribution for eMRTDs.

How so, you may ask?

71. How is PKI used in eMRTDs

eMRTD TRUST MODEL

Consider the ePassport trust model.

The Country issuing the ePassport will first create a self-signed certificate. This self-signed certificate is the Root of Trust in the country and is called the Country Signing Certificate Authority (CSCA). This CSCA is distributed to all the other countries that wish to verify this ePassport.

To sign the passports, the country generates additional key pairs that are then used to create certificates that are signed by the CSCA. These certificates are called Document Signer Certificates (DSCs). The DSC is then used to sign the passport contents (This is covered in section 56: “How are eMRTDs verified” in greater detail), and the DSC is also included in the passport.

The entity verifying the passport uses the DSC in the passport to verify the contents of the chip. They then verify the DSC using the CSCA that was previously received from the country. How does this help us?

Consider the following:

- The CSCA is used to issue only DSCs. A DSC is only generated once every 3 months or so, which means that

it does not need to be online. This means that CSCA may be housed in a secure room with no network connections and with a strict physical access policy to prevent theft, loss or compromise of the Private Key

- DSC is used for a very limited time (usually 3 months) and then the Private Key is destroyed. This limits the possibility of a key compromise. Using a different DSC every few months does not required distribution as it is included in the chip of the eMRTD.

But, if the DSC does get compromised, eMRTDs signed by the DSC cannot be fully trusted. How do you inform verifiers of this DSC compromise?

A Certificate Revocation List (CRL) is a structure that contains the details of the DSCs that are compromised and is signed by the CSCA. The process of verification of an eMRTD must also check the CRL to ensure that the DSC is not on the revoked list.

But we still haven't explained the difference between Public Key Cryptography and Public Key Infrastructure.

Generating the CSCA and then using it to issue DSCs and CRLs requires a set of policies, hardware, software and operations procedures to manage the process.

This infrastructure that allows for such key management is called Public Key Infrastructure (PKI).

So, when we mention the eMRTD PKI, it encompasses the infrastructure to issue and manage CSCAs, DSCs, CRLs along with the 2-tier trust model and associated processes that are based on Public Key Cryptography.

The eMRTD trust model is the same whether you are issuing passports or ID cards with a chip in them. Additionally, there are some important points to remember.

The Document Signer Certificate (DSC) has a specific profile defined depending on the use case. A profile is the mandatory fields that must be present in the DSC. These fields help to differentiate the intended use of the DSC.

CERTIFICATE REVOCATION LIST

PUBLIC KEY INFRASTRUCTURE

IS THE MODEL SAME FOR eIDs?



The DSC used for eMRTDs and DSC used for eIDs have different mandatory fields. This is to ensure that DSCs are used for the purpose they were intended for. A DSC issued to sign eMRTDs must sign eMRTDs only, while a DSC issued to sign and eID must sign eIDs only.

72. The contents of the chip

WHAT IS IN THE CHIP?

The chip contains the biographic and biometric information of the traveller. The chip has a file structure. This is similar to how files are organised in a hard disk. The files in the chip are called Elementary Files (EF). Each of the EFs have a specific tag number which can be used to select and read them. The contents of the EFs are defined as data groups (DGs).

There are 16 data groups that are defined in ICAO Doc 9303.

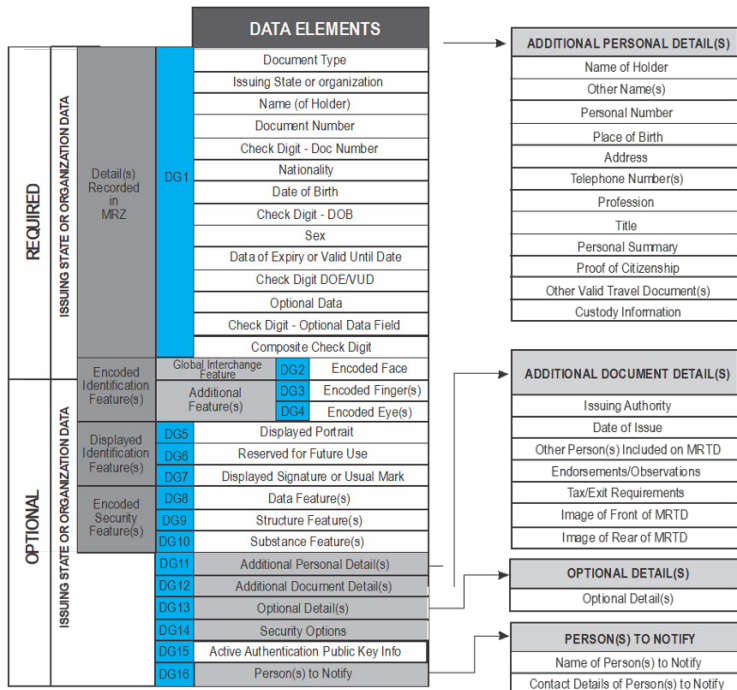


Figure 24 - eMRTD Chip Datastructure / Datagroups

The contents of the data groups are as follows:

- Machine Readable Zone
The contents of the MRZ are reproduced in DG1.
DG1 is mandatory
- Encoded face
The image of the holder is stored in DG2. It is not a template but an actual image. DG2 is mandatory
- Encoded fingers
An image of one or more fingerprints of the traveller may be stored in DG3. DG3 is optional.
- Encoded irises
An image of one or two IRIS images may be stored in DG4. DG4 is optional.
- Displayed portrait
DG5 is optional
- Reserved for future use
DG6 is not currently used.
- Displayed signature or usual mark
An image of a signature or any identifying mark of the person. DG7 is optional
- Data features
DG8 is not yet defined
- Structure features
DG9
- Substance features
DG10
- Additional personal details
DG11
- Additional document details
DG12

- Optional details
[DG13](#)
- Security options for secondary biometrics
[DG14](#)
- Active Authentication Public Key info
[DG15](#)
- Persons to notify
[DG16](#)
- Security Data Object
[SOD](#) – This is covered in [section 56: “How are eMRTD verified”](#).

PROTECTING THE DATA IN THE CHIP

The data in the chip is protected using Public Key Cryptography. It facilitates tamper detection, but does not offer tamper protection. This means that it is possible to detect that the data in the chip has been fraudulently changed, but it cannot prevent such changes. That is why, proper validation of the chip contents is necessary. Read more about this in [chapter 11: “Document verification”](#).

A possible fraud scenario is the cloning of the [eMRTD](#). A clone is a copy of the [eMRTD](#). This can be used for lookalike fraud, where two persons who resemble each other carry two copies of the same document issued to one of them. To detect such cloning, there are two protection mechanisms. They are:

- Active Authentication ([AA](#))
- Chip Authentication ([CA](#))

The chip has a Private Key that is stored in a secure area inside the chip. The Public Key is stored in Data Group 15 as mentioned above. The secure area cannot be cloned.

The Inspection system sends a random challenge for the chip to sign using its Private Key. It then attempts to verify the response using the Public Key in [DG15](#). If it succeeds, then the chip can be trusted as being the original chip and not a clone. The two mechanisms ([AA/CA](#)) differ in the cryptographic algorithms and keys used. The underlying principle is the same.

CHAPTER 15

BIOMETRICS



What you will learn about in this chapter:

- Understand the types of biometrics used in ID and travel documents
- Understand the implications for choosing the right type of biometrics for use in ID credentials

73. A brief introduction to biometric identification

Biometric identification describes the recognition or identification of a person through the process of matching to a pre-registered biometric information. If the biometric is the face, this can be done by visual comparison. However, it is generally used to describe a machine assisted process of recognition or identification.

During registration, the biometric of the person is captured and converted to a template and stored in a reference database. A biometric template is a digital reference of distinct characteristics that have been extracted from a biometric sample.

In the process of recognition or identification, the biometric is again captured, turned into a template and a software algorithm then compares it to the stored template and returns a confidence level as to how close the two templates are to each other.

The algorithm to create the template is different for different manufacturers of such software and these are not generally interoperable. So, it is best to store the biometric information as a high-quality image, and then do the conversion to template at the point of biometric matching. In deciding the type of biometric to be used in ID and travel documents, key considerations are:

Interoperability

Biometrics that are stored in the document must be readable and usable across different systems.

Reliability

The biometric technology must have been proven to ensure a high standard of reliability in biometric identification. Many technologies exist and are being developed, but their use in travel and identification must be done only if the accuracy and reliability of such systems can be guaranteed.

Viability

The technology must be viable for deployment. Some technologies require highly sophisticated mechanisms for

both enrolment and verification, but the deployment of such technology may not be viable, especially in a border control environment.

One-to-one versus one-to-many

The data quality and technology must be fit to operate in the designated mode. Verifying the identity of a person versus a presented document will have lower requirements than matching a person versus a database of biometrics. Such a search could be required during the issuance of documents, making sure the person has a unique identity. Or matching against wanted-persons-database. This later case is especially important when the FMZ-agreement foresees the processing of legal status in one country, valid for all the territory.

74. Types of biometrics used in travel documents

There are dozens of biometrics available to identify persons. However, ICAO Doc 9303 considers only three types of biometric identification systems for the use of traveller identification. These biometrics are stored in Data Groups on the eMRTD as introduced in chapter 14: “PKI and the chip in travel documents” where we introduce you to the basics of the chip data structure:

Facial recognition is the matching of the face captured from a camera against a reference image. The reference image is stored in Data Group 2 of the eMRTD. This biometric is mandatory.

FACIAL
RECOGNITION

Fingerprint recognition involves the comparison of the friction ridges between a presented finger and the stored image. Countries freely choose how many and which fingerprints will be captured. Many go for two-index, index and thumbs or all ten fingerprints. The reference image is stored in Data Group 3 of the eMRTD. This biometric is optional.

FINGERPRINT
RECOGNITION

Iris recognition uses a high-resolution image of the Iris of the person to carry out the biometric matching. This can be in the visible spectrum or near infra-red light spectrum. The reference image is stored in Data Group 4 of the eMRTD. This biometric is optional.

IRIS RECOGNITION

CHAPTER 16

LINKING OF IDENTITIES WITH PEOPLE



The process by which a state establishes and verifies a person's identity before issuing an identity document to them are important in their own right. It becomes all the more important when multiple states get together to form a Free Movement Zone.

This chapter gives an overview of the principles that may be used to establish the identity of a person.

75. Evidence of Identity

“ Be yourself; everyone else is already taken. ”

— Oscar Wilde

Accurate establishment of a person's entitlement to a claimed identity is crucial for any identity system.

The identity of a person is usually established using foundational documents like birth certificates or death certificates. Such information may reside in a civil registry.

Some key points are summarized here:

Traditionally, identity is established in a relatively linear manner starting with a foundational record like a birth certificate. Subsequent identity documents are all linked to this foundational document and ends with the closure of the identity.

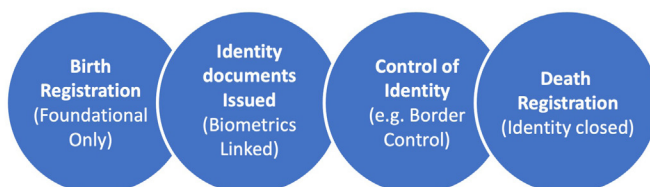


Figure 25 - Establishment of Identity (Linear representation) |
© ICAO Guide on Evidence of Identity

If fraud occurs anywhere in this linear process, it is propagated throughout the rest of the lifecycle of the identity.

However, the Evidence of Identity (EOI) approach evaluates the Identity Context and proposes a risk based approach to evaluate every piece of evidence that is used to establish an identity.

Broadly speaking, it proposes three objectives

- Claimed Identity is genuine.
- Presenter links to the Identity.
- Presenter uses the claimed identity.

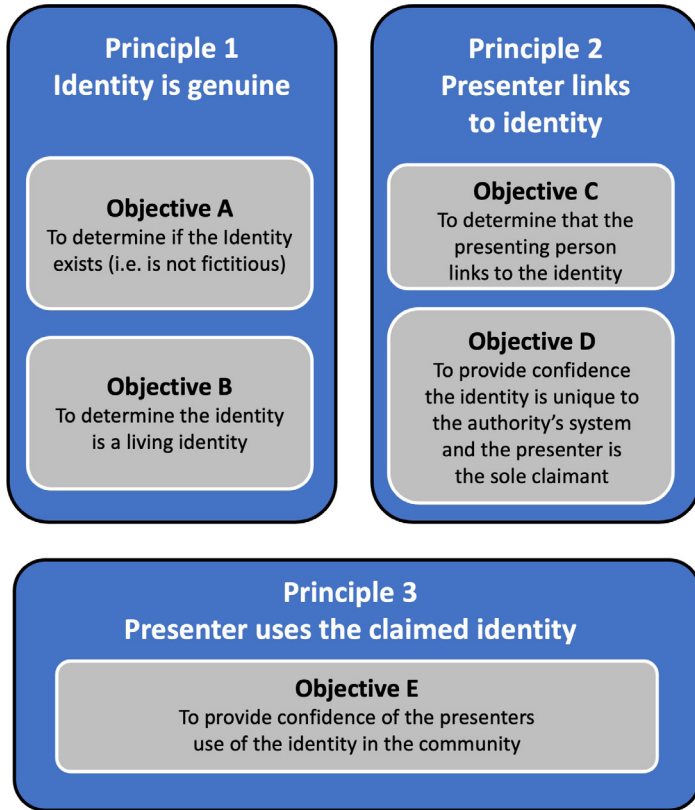


Figure 26 – Principles for establishing “Evidence of Identity” | ©ICAO Guide on Evidence of Identity

The above is only a very high-level abstract. A very good guidance material on this subject can be found in the “ICAO Guide on Evidence of Identity”.

<https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/ICAO%20Guide%20on%20Evidence%20of%20Identity.pdf>



76. How to make sure that people don't acquire multiple identities

Accurate establishment of a person's entitlement to a claimed identity is crucial for any identity system.

An important aspect to note is that for travel purposes ICAO requires that one person should be able to claim only one identity. If a person is able to claim multiple identities, different identities could be used for fraudulent or criminal activity.

An effective way of ensuring that the claimed identity is unique is the use of biometrics.

If biometric data is gathered as part of both the civil registry and any additional identity management system such as a national population register or national ID card scheme, a one-to-one match can be done to establish the identity of the applicant. A one-to-many biometric match will help in identifying any attempts to claim multiple identities by the same applicant.

CHAPTER 17

UPINs – CONSIDERATIONS ON HARMONIZATION



What you will learn about in this chapter:

- What are UPINs
- Why should we be interested in them in this context
- Where to find additional supporting resources

77. What are UPINs

UPIN is an acronym for Unique Personal Identification Number. In much of the literature you will find the shorter acronym UIN, which stands for Unique Identification Number. The authors prefer to add the “personal” to the definition, as we want to focus on the person, and not on a data record or document. This is a number uniquely and permanently attributed to an individual and serves to link a data record to this individual. The number often is assigned during the process of birth registration and remains assigned even beyond death.

Having a UPIN is beneficial for individuals as a means to be recognized for who they are and access ascribed benefits and rights, including, for example, accessing education, registering to vote or the act of voting, opening a bank account, buying or inheriting property, paying taxes, enrolling in a health insurance plan, and qualifying for a cash transfer. It is also an important tool for governments to ensure that the right person has access to an ascribed service.

UPINs are an important instrument within each country, and so it is usually designed to the national needs. In the context of FMZs, there is a need for some interchangeability on these identifiers. We will look into this in greater detail below.



A very dense and helpful guide on the subject of UPINs, including an overview of the implementations across the world is provided by the World Bank Group:

“Integrating Unique Identification Numbers in Civil Registration”, World Bank Group, Washington, 2018

<https://documents.worldbank.org/en/publication/documents-reports/documentdetail/674401531758210363/integrating-unique-identification-numbers-in-civil-registration>

78. Is there a need for a uniform, inter-operable UPIN for the region

The UPIN is a successful tool in managing civil registries and population registers. This is discussed above. When societies 'merge' beyond just simple travel, however, it might be a good topic to discuss, in the multi-lateral working groups of the involved nations to the FMZ whether there is a need for a uniform UPIN for the region. In order to support this discussion, we will highlight three scenarios:

When citizens of another country enjoy extended freedom, there arises the need to manage and sometimes to investigate. There will be situations when data needs to be exchanged or even updated. With independent unique identifiers such as UPINs, the data exchange will require a translation table. Less errors and better response times could be expected with harmonized UPINs.

ACCESSIBILITY TO
DATA

Vital events such as birth, death and marriage can take place abroad, and even more so when the FMZ is attractive to the population. Capturing the identifiers in the various forms and processes, and tracking these through the national and international systems, can require adaptations to the systems. Identity verification and near-real-time updates preventing abuse and fraud can be considerably hindered.

VITAL EVENTS

Especially when Visa unions are established, management of identity and avoidance of unauthorized multiple-nationalities become key. A uniform UPIN is one of the building blocks of getting a grip on this.

MULTIPLE
IDENTITIES

In regions, where the countries already use a system like UPINs, the price of migrating and merging the systems might be a price too high to pay for the potential benefits. For regions without a system already established, considering a common approach might be a big plus.

The European Union did not introduce a common UPIN system. All member countries maintained their own system. Also, the whole civil registration systems still follow different policies, which didn't make a migration of systems a viable and crucial activity.



ANNEX 2

ACRONYMS AND MORE



79. Acronyms and glossary

2D	Two dimensional (as in 2D-Barcode)
3D	Three dimensional
AA	Active Authentication (→ page 147)
ABC	Automated Border Control (→ page 145)
ABS	Acrylonitrile butadiene styrene
AfCFTA	African Continental Free Trade Agreement
AI	Artificial Intelligence
API	Advance Passenger Information. https://www.icao.int/Security/FAL/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards.aspx
ASEAN	Association of Southeast Asian Nations
BAC	Basic Access Control (→ page 113)
BCM	Border Control Management
CA	Chip Authentication (→ page 147)
CARICOM	Caribbean Community (→ page 45)
CAN	Card Access Numbers (→ page 113)
CMYK	Cyan-Magenta-Yellow-Black
COMESA	Common Market for Eastern and Southern Africa
CPTPP	Comprehensive and Progressive Trans-Pacific-Partnership
CRL	Certificate Revocation List (→ page 167)
CSCA	Country Signing Certificate Authority (→ page 166)
CTA	Common Travel Area (→ page 43)
D2T2	Dye-Diffusion-Thermal-Transfer (→ page 86)
DB	Database
DG	Data Group (→ page 168)
DOVID	Diffraction Optically Variable Image Device
DSC	Document Signer Certificates (→ page 166)
DTA	Digital Travel Authorization (→ page 95)
DTC	Digital Travel Credentials (→ page 79)

EAC	Extended Access Control
EAC	East African Community
ECOWAS	Economic Community of West African States
EDISON TD	Electronic Documentation Information System on Network - Travel Documents (→ page 131)
EF	Elementary File (→ page 168)
eID	electronic identity document
eMRTD	electronic Machine-Readable Travel Document
EOI	Evidence of Identity (→ page 176)
EU	European Union
FADO	False and Authentic Documents Online (→ page 131)
FAST	The Free and Secure Trade (FAST) programme is a commercial clearance programme for known low-risk shipments entering the United States from Canada and Mexico. Initiated after 9/11, this innovative trusted fulfiller/trusted shipper programme allows expedited processing for commercial carriers who have completed background checks and fulfil certain eligibility requirements. https://www.cbp.gov/travel/trusted-traveler-programs/fast
FR	Facial Recognition
FMZ	Free Movement Zone (→ pages 20, 27)
GDP	Gross Domestic Product
iAPI	Interactive Air Passenger Information. The Interactive Advance Passenger Information (iAPI) provides opportunities for governments to communicate an instant response to carriers based on vetting results. This information helps airlines determine whether or not passengers have the appropriate travel document and requirements in order to enter the country of destination (i.e. Visa). https://www.icao.int/Security/FAL/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards.aspx
IATA	International Air Transport Association; https://www.iata.org
ICAO	International Civil Aviation Organization; https://www.icao.int/Pages/default.aspx
ICBWG	Implementation Capacity Building Working Group (→ page 117)
IOM	UN International Organization for Migration https://www.iom.int/

IR	Infra-Red
ISO	International Standards Organization
LDS	Logical Data Structure (→ page 115)
mDL	mobile Driving License
MRZ	Machine Readable Zone
NEXUS	The NEXUS programme allows pre-screened travellers expedited processing when entering the United States and Canada. Programme members use dedicated processing lanes at designated northern border ports of entry, NEXUS kiosks when entering Canada by air and Global Entry kiosks when entering the United States via Canadian Preclearance airports. NEXUS members also receive expedited processing at marine reporting locations. https://www.cbp.gov/travel/trusted-traveler-programs/nexus
NTWG	New Technologies Working Group (→ page 117)
OCR	Optical Character Recognition (→ page 91)
OS	Operating System
OTA	Over the air
OVD	Optical Variable Device (→ page 104)
PIK	Primary Inspection Kiosk (→ page 144)
PACE	Password Authenticated Connection Establishment (→ page 113)
PC	Polycarbonate (→ page 88)
PET	Polyethylene Terephthalate
PKC	Public Key Cryptography (→ pages 146, 161)
PKD	Public Key Directory (→ page 135)
PKI	Public Key Infrastructure (→ page 163)
PNR	Passenger Name Record: https://www.icao.int/Security/FAL/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards.aspx
PRADO	Public Register of Authentic travel and identity documents online (→ page 132)
PVC	Polyvinyl Chloride (→ page 87)
QR	Quick Response Code
REC	Regional Economic Community
RTA	Regional Trade Agreement (→ page 22)

SADC	Southern African Development Community
SARPs	Standards and Recommended Practices. The safety management SARPs are intended to assist States in managing aviation safety risks, in coordination with their Service Providers. Given the increasing complexity of the global air transportation system and its interrelated aviation activities required to assure the safe operation of aircraft, the safety management provisions support the continued evolution of a proactive strategy to improve safety performance. The foundation of this proactive safety strategy is based on the implementation of a State safety programme (SSP) that systematically addresses safety risks, in agreement with the implementation of the safety management systems (SMS) by the service providers.
SENTRI	The Secure Electronic Network for Travelers Rapid Inspection (SENTRI) is a U.S. Customs and Border Protection (CBP) programme that allows expedited clearance for pre-approved, low-risk travellers upon arrival in the United States. Participants may enter the United States by using dedicated primary lanes into the United States at Southern land border ports. Travelers must be pre-approved for the SENTRI programme. All applicants undergo a rigorous background check and in-person interview before enrolment https://www.cbp.gov/travel/trusted-traveler-programs/sentri
SCHENGEN AREA	EU Member States: Belgium, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxemburg, Malta, The Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Tchechia). Outside the EU: Iceland, Liechtenstein, Norway, Switzerland
SOD	Security Data Object (→ page 134)
SLTD	Interpol Stolen and Lost Documents Database
TAG	Technical Advisory Group
TRIP	Traveller Identification Programme
UIN	Unique Identification Number (→ page 180)
UPIN	Unique Personal Identification Number (→ page 180)
UV	Ultra Violet
VDS	Visual Digital Seal (→ page 79, 93)
VDS-NC	Visible Digital Seal for Non-Constrained environments (→ pages 79, 94)
VIS	EU Visa Information System
WTO	World Trade Organisation.

80. Stakeholders

Below lists a number of stakeholders respectively roles that you might want to consider when preparing for an FMZ. This list is not complete, and will need adaptation to your specific situation, objective and context.

Subject	Aspects and Stakeholders
Politics and Citizens	<ul style="list-style-type: none"> <input type="checkbox"/> Elements of the State system (e.g., Presidents Office, Ministers, Parliament) <input type="checkbox"/> Political parties <input type="checkbox"/> Expert agencies handling objectives, Trade-offs and impact on ongoing businesses and treaties
	<ul style="list-style-type: none"> <input type="checkbox"/> Sub-national authorities in general, and especially near the borders, economic hubs and regions that might be economically impacted by changed competitive situation (e.g., agricultural areas)
	<ul style="list-style-type: none"> <input type="checkbox"/> Foreign Affairs <input type="checkbox"/> Stakeholders of treaties and developing business with the FMZ-Candidate Countries <input type="checkbox"/> Counsellor services in the FMZ-countries
	<ul style="list-style-type: none"> <input type="checkbox"/> Buy-in of the citizens into the idea <input type="checkbox"/> National identity requirements <input type="checkbox"/> Representative of tribes or groups with frequent border crossings or traditional rights possibly impacted <input type="checkbox"/> Associations for special needs groups
	Legal
<ul style="list-style-type: none"> <input type="checkbox"/> Data protection authorities <input type="checkbox"/> Civil rights protection groups 	
<ul style="list-style-type: none"> <input type="checkbox"/> Ethics commissions 	
Financial and Economy	<ul style="list-style-type: none"> <input type="checkbox"/> Ministry of Finance/Budgeting and Financing of the project <input type="checkbox"/> Agency for customs-affairs <input type="checkbox"/> Taxation of foreigners
	<ul style="list-style-type: none"> <input type="checkbox"/> Ministry of Economy/Agency for economic affairs <input type="checkbox"/> Research agencies and universities: Economic impact modelling, projection and management of the FMZ <input type="checkbox"/> Ministry of infrastructure and strategic development
	<ul style="list-style-type: none"> <input type="checkbox"/> Tourism association
	<ul style="list-style-type: none"> <input type="checkbox"/> Business-associations <input type="checkbox"/> Traveler organizations and related industry <input type="checkbox"/> Airline operators

Subject	Aspects and Stakeholders
Education and Work	<ul style="list-style-type: none"> <input type="checkbox"/> Handling of faculty and student exchange <input type="checkbox"/> Acknowledgement of certifications <input type="checkbox"/> Studies on relationships and impacts; Freedom and Politics faculties <input type="checkbox"/> Ministry for education
	<ul style="list-style-type: none"> <input type="checkbox"/> Handling the affairs of national and international employment <input type="checkbox"/> Working permits <input type="checkbox"/> Trade Unions and associations/representatives of industries / farmers <input type="checkbox"/> Worker-NGOs / Workers' Relief Associations
	<ul style="list-style-type: none"> <input type="checkbox"/> Social Insurance agencies <input type="checkbox"/> National statistics bureau
Security and Migration	<ul style="list-style-type: none"> <input type="checkbox"/> Agencies handling national security interests, including domestic and international crime, information exchange <input type="checkbox"/> Border police <input type="checkbox"/> National Police Authorities <input type="checkbox"/> National Law Enforcement Agencies
	<ul style="list-style-type: none"> <input type="checkbox"/> Migrant agencies <input type="checkbox"/> Migrant rights organisations
	<ul style="list-style-type: none"> <input type="checkbox"/> Considerations of the armed forces on national security <input type="checkbox"/> Impact on logistics and scenario preparations <input type="checkbox"/> Joint operations or possible defence unions
	<ul style="list-style-type: none"> <input type="checkbox"/> Civil Registration and Public Registry offices <input type="checkbox"/> Association of notaries <input type="checkbox"/> Hospitals, birth centers and related associations for birth/death registrations
	<ul style="list-style-type: none"> <input type="checkbox"/> Issuance Organisations <input type="checkbox"/> State Printers <input type="checkbox"/> National IT Service provider <input type="checkbox"/> Certificate Authority <input type="checkbox"/> Cyber Security Specialists <input type="checkbox"/> National Database operators (e.g., Criminal Records, National Intelligence, Persons Registry etc)
	<ul style="list-style-type: none"> <input type="checkbox"/> Airport Authorities <input type="checkbox"/> Seaport Authorities <input type="checkbox"/> Trans-Border operating Train and Bus Operators

Table 11 - List of stakeholders

81. Tables

Table 1	Checklist with Priority of interests
Table 2	Checklist with fields potentially subject to harmonization
Table 3	Checklist of potential beneficiaries of FMZ border crossing
Table 4	Matrix visualizing the connections between data-carrier technologies, required readers and suitable documents as technology carriers
Table 5	Checklist: Preparing for the Design of the FMZ-credential
Table 6	Checklist: “Designing a harmonized security concept”
Table 7	Checklist: “Intelligent Security Concepts”
Table 8	Checklist: Considerations for non-physical credentials
Table 9	Checklist: Validation of passport documents
Table 10	Checklist: Validation of non-passport documents
Table 11	List of stakeholders

82. Figures

Figure 1	Chart explaining the principle of an Investment Logic Map
Figure 2	Stakeholder groups for consideration in the process. A more detailed listing is provided in section 80: “Stakeholders”.
Figure 3	Swiss ePassport Datapage ©Council of the EU, Database: Prado
Figure 4	Singapore ePassport Datapage with integrated Chip ©Council of the EU, Database: Prado
Figure 5	Portuguese ePassport Datapage ©Council of the EU, Database: Prado
Figure 6	Subset of OCR-B Characters from ISO/IEC 1073-2 for use in machine readable travel documents (From ICAO Doc 9303)
Figure 7	A passports machine readable zone (MRZ) explained; ©ICAO Doc 9303
Figure 8	Sample 2D-Codes: QR-Code, Datamatrix, Aztec-Code

- Figure 9 Data elements in a visual digital seal (VDS); ©ICAO Doc 9303
- Figure 10 Schema of the electrical functioning of a contactless Interface
- Figure 11 Zones on recto and verso of an ID-1 format ID-card; ©ICAO Doc 9303
- Figure 12 Spanish, Swiss and Chilean ID cards ©Council of the EU, Database: Prado; Ghana ID card ©National Identification Authority Ghana
- Figure 13 Structure of the Logical Data Structure and the Security Data Objects | ©ICAO
- Figure 14 Visualization of the complexity of having only bilateral DSC and CRL exchanges versus using the PKD for distribution. | ©ICAO
- Figure 15 Samples of PIKs | ©CBSA-ASFC. | <https://www.cbsa-asfc.gc.ca/travel-voyage/pik-bip-eng.html>
- Figure 16 User-experience and process steps during the operation of an eGate
- Figure 17 ABC-gate monitoring in command centre ©Figure by authors. Photo of ABC gate: Elliott Killingbeck https://commons.wikimedia.org/wiki/File:GAT_South_eGates.JPG
- Figure 18 The input length of the message has no effect on the resulting hash
- Figure 19 Avalanche effect of hashing message with minimal deviations
- Figure 20 Principle of Cesar Cypher with a shift of 3 (Rot3)
- Figure 21 Cesar Cipher Encoding Table with Rot3
- Figure 22 Cesar Cipher Encoding Table with Rot3
- Figure 23 Visualization of a Digital Certificate
- Figure 24 eMRTD Chip Datastructure / Datagroups
- Figure 25 Establishment of Identity (Linear representation) | ©ICAO Guide on Evidence of Identity
- Figure 26 Principles for establishing “Evidence of Identity” | ©ICAO Guide on Evidence of Identity

