Universiteit Leiden
The Netherlands

What Was the Effect of the Implementation of an RFID-chip in Passports on the Rate of Detected Identity Fraud in the Netherlands?

Hoorn, Marleen

Citation
Hoorn, M. (2022). *What Was the Effect of the Implementation of an RFID-chip in Passports on the Rate of Detected Identity Fraud in the Netherlands?*.

Version:	Not Applicable (or Unknown)
License:	License to inclusion and publication of a Bachelor or Master thesis in the Leiden University Student Repository
Downloaded from:	https://hdl.handle.net/1887/3281517

Note: To cite this publication please use the final published version (if applicable).

What Was the Effect of the Implementation of an RFID-chip in Passports on the Rate of Detected Identity Fraud in the Netherlands?

Name: Marleen Hoorn
Student Number: s3001814
Master Program: Economics & Governance / Public Administration
Date: January 9, 2021
Capstone: Technology in the Public Sector
Professor: M. Young
Word Count Whole Document: 21672
Word Count Excluding References: 16580
Number of Pages: 82

Key words: Identity Fraud, RFID, Biometrics, E-passports, Look- alike fraud, Chip

Executive Summary

The purpose of this dissertation, conducted at Leiden University is to research the effect of the implementation of an RFID chip in passports on the rate of detected identity fraud in The Netherlands.

In order to answer the main research question, different research methods were chosen. Desk research was used for the literature study which provides the background information of this thesis. The results are also based on desk research because the data from annual statistical reports were used. Field research was conducted through an interview with two employees from the data providing institution.

The research showed that the implementation of RFID chips in passports created security and privacy issues that entail many dangers. On the other hand, the addition of biometric data on the chip brings great benefits. In the results, in which the data from the annual reports of the expertise center for document fraud in the Netherlands has been analysed, it is clear that no major reduction in the size and modus operandi of committed identity fraud is visible. This led to the conclusion that the chip's implementation has had no major effect on the magnitude and nature of identity fraud.

Table of Contents

Preface

This Master Thesis is created in as part of the Master program Economics & Governance at Leiden University. I would like to thank professor Young from the university for his supervision, input, and feedback. In addition, I would like to thank Ms Lonneke Bontje and Mr Castanon of the expertise center for identity fraud for their time and cooperation on the thesis.

Introduction

As a result of the 9/11 attacks, the United States required that countries wishing to continue participating in the visa waiver program provided their citizens with machine-readable travel documents (MRTDs) containing digital photos. The European Union (EU) has complied with this and set 28 August 2006 as the deadline for implementation. Additionally, the EU had also decided to include biometrics in its passports (Schouten, 2008). The purpose of biometric passports is to prevent the illegal entry of travellers into a particular country and limit the use of false documents (Kosmerlj, 2005). Currently, more than 100 countries use e-passports. These types of documents are believed to be the most reliable methods of identification because they are based on the biometric features of a person that make this individual unique. Therefore, they can be used for identification and authentication (Bobkowska, 2019).

Passports with RFID chips were first approved by the Malaysian government in 1998. However, until 2002, these passports did not meet the basic security requirements. The information on the passport holder's chip was not encrypted. The only measure to secure the data on the chip was a digital signature that ensured that the information could not be changed by unauthorized persons. This measure was largely inadequate as it did not prevent passports from being cloned or skimmed (Nithyanand, 2009). Later in 2004, the International Civil Aviation Organization (ICAO) drew up the guidelines for e-passports and other travel documents with RFID functionality (A. Juels, 2006).

Research Question

The ICAO has set security goals for e-passports, which include data integrity, mutual authentication, and non-repudiation (Nithyanand, 2009). This study aims to answer what the effect is of the implementation of RFID chips in passports on the rate of detected identity fraud in The Netherlands. Therefore, it is important to check whether the ICAO security goals have been achieved and whether the ICAO guidelines were and are sufficient to guarantee the safety of e-passports. Hence, the main research question is formulated as follows:

"What Was the Effects of the Implementation of an RFID-chip in Passports on the Rate of Detected Identity Fraud in The Netherlands?"

This RFID chip contains biometric data of the passport owner and therefore the impact of the implementation of biometric data on e-passports is also being investigated. To answer the main research question, several sub-questions will be answered, which contribute to answering the main question. These sub questions are:

- *What are the strengths and vulnerabilities of e-passports?*
- *What types of identity fraud do exist?*
- *What are the consequences of adding biometric data to RFID chips in passports?*

Scope

This research report will focus specifically on identity fraud committed on Dutch territory. This country was chosen because the Netherlands, unlike many other countries, is transparent in the field of identity fraud. The figures of identity fraud on Dutch territory are updated annually and published in a statistical report. In these reports, a distinction is made between all documents that have been intercepted and specifically the fraud involving Dutch documents. Because the implementation date of e-passports is not exactly the same for every country, the data on document fraud involving identity documents from around the world will be compared with the specific data regarding Dutch documents.

Academic relevance

The main reason for introducing e-passports with biometric data was mainly to combat the so-called phenomenon of "look-a-like fraud". The American government suspects that mainly terrorists are engaged in this form of identity theft. Due to the increasing threat of terrorism, it was therefore important to find a solution to identity fraud committed with passports. The introduction of a passport with a chip on which biometric data was implemented, which can be used to check whether the user of the passport is also the rightful owner, was seen as a good solution to the problem. Despite the promising technology, the e-passport was and still is under fire from privacy advocates and security experts. According to them, there are also dangers associated with the introduction of e-passports. Criminals could, for example, steal passport details which is not in line with the goal to decrease terrorism and identity fraud. The RFID technology must be used to combat terrorism, but it can actually help terrorists achieve their goals (A. Juels, 2006).

Much research has been done on the pros and cons of e-passports and in particular their safety and security, however the literature does not elaborate on the magnitude of the impact of e-passports on identity fraud. This phenomenon is actually still unexplored, and this research has been conducted to change that. The research answers the question what the effect of the implementation of the e-passport is, so that it can be concluded whether the e-passport has contributed to the fight against identity fraud.

Societal Relevance

Due to the digitizing world, safeguarding people's privacy plays an increasingly important role in our daily lives. The provision of biometric data such as fingerprints and iris scans, is a sensitive topic nowadays. The question of whether the benefits of implementing biometric data on passports outweigh the privacy that citizens must give up is an increasing issue. By investigating the impact of the implementation of RFID chips with biometric data on passports, it can be concluded whether the privacy that citizens surrender actually outweighs the benefits.

Method of data collection

The research question of this report will be answered through data analysis from the statistical annual overviews of the Expertise Center for Identity Fraud and Documents (ECID). These reports contain specific figures about all kinds of fraud with (Dutch) Identity Documents. These numbers will be visualized in tables and graphs. Subsequently, an analysis, in combination with an interview with two ECID employees, will conclude what the effect of the introduction of RFID chips with biometric data on identity fraud has been.

Summary

After this introductory chapter, in which the main and sub-questions are explained and the academic and societal relevance of the subject is described, the following chapter contains the literature review with all relevant background information. It becomes clear that there are many security and privacy issues associated with the use of RFID chips with biometric data in passports. Subsequently, in the results chapter, the statistical annual reports of the ECID are analysed and it becomes clear that there is no significant impact on identity fraud noticeable based on this data.

Finally, in the discussion chapter, it will become clear whether the research can be generalized, whether the hypotheses have been confirmed or disproved and what the limitations of the research were.

Background Information

This report focuses on answering the question what the impact is of the implementation of Radio Frequency Identification (RFID) chips in passports. A passport in which an RFID tag with relevant biometric information of the owner is implemented is called an electronic passport or e-passport (Nithyanand, 2009). The ICAO (International Civil Aviation Organization) has called on countries to implement these chips in passports. The ICAO is a body of the United Nations with the authority to set international passport standards (Juels et al., 2005). The three constituent technologies in e-passports are biometrics, public key infrastructure and RFID. They help to deal with user authentication and fraud management problems (Nithyanand, 2009). Those technologies will be defined and explained in this literature review. As the beginning of this literature review, it is important to clarify the difference between identification, authentication and legitimation because these terms are common in this study. Identification is establishing someone's identity to verify that someone is actually who they say they are. Authentication is determining whether someone can be granted access on the basis of an identity or derived identity (such as an access pass, account or token). Legitimation is determining whether the person who shows an ID device is authorized to do something (Brummelkamp, 2020).

Identity

Every person has all kinds of different characteristics that distinguish him or her as an individual from others. These can be biometric properties or personality. Personal traits are not visible outwardly, they are character traits that are often linked to a certain type of personality, which are expressed in the behaviour of an individual (Williams, 1956). Biometric traits are most of the time outwardly visible and these body features are unique. Some biometric traits require technologies to see them, this applies to for example DNA and fingerprints, but all biometric traits are unique. The whole or parts of these distinctive features are called an identity (Ministerie van Binnenlandse Zaken en Koninklijksrelaties, 2013). However, the precise definition of what identity is will differ from situation to situation. The government assigns citizens a formal identity that is used in a broader context than just government services. At the same time, citizens also have various private identities with which they identify themselves for companies (Ministerie van Binnenlandse Zaken en Koninklijksrelaties, 2013).

Christopher Williams claims that the concept of identity leads to a paradox. He says: "we cannot truly and usefully say that a thing is the same either as itself or as something else" (C.J.F. Williams, 1989, p. 86). Moreover, the concept of identity is often defined very differently. Brief definitions and clarifications regarding the concept of identity can be found in many sources. These definitions range from succinct suggestions to rather complicated and opaque formulations. Hogg and Abrahams (1988) define identity as people's concept of who they are, of what sort of people they are, and how they relate to others. This definition refers to how people see themselves and each other and is very similar to the definition of identity from Francis Deng. Deng (1995) defines identity as the way individuals and groups define themselves and are defined but others on the basis of race, ethnicity, religion. language and culture (Deng, 1995).

This study goes with the definition of the concept 'personal identity' to clearly define what is meant by identity. According to Max Haller and Bernadette Müller, personal identity refers to the uniqueness of an individual that emerges on the basis of identity tags (name, biometric features, characteristics) and the individual biography (Müller, 2008).

RFID

Radio-Frequency Identification (RFID) technology is a wireless sensor technology based on the detection of electromagnetic signals (Domdouzes et al., 2007). An RFID system consists of three components. These are an antenna that transmits radio signals, a transceiver with decoder (which is responsible for receiving the data), and a transponder (RF tag) that is electronically programmed with unique information. The radio signals emitted by the antenna activate the tag that reads the data. The antenna is thus responsible for communication between the tag and the transceiver (Domdouzes et al., 2007). From a physical point of view, an RFID tag is a small microchip attached to an antenna (this antenna is used to both send and receive a signal). An RFID tag often looks like a kind of self-adhesive sticker. An RFID chip, on the other hand, is many times smaller (Atzori et al., 2010). RFID is a promising technology that will undoubtedly simplify various everyday operations in the future and lead to many new applications. However, these new possibilities are not without risk because a lot of action and control is required in terms of privacy and security in order to work seamlessly with devices with RFID technology (Bocchetti, 2006).

RFID and biometric technologies promise to reduce fraud, make identity checks easier and improve security (Juels et al., 2005). However, as mentioned before, these technologies also pose new risks. This is endorsed by many other researchers, including Professors Atkins and Yu. They claim that the use of an RFID tag can lead to a violation of the privacy of citizens who have the tag implemented in their passport (Atkins & Yu, 2011). Because the RFID tag has a unique identification number, it is subject to various security and privacy risks, such as the traceability of a person, the leakage of information and the imitation of a chip (Atkins & Yu, 2011). In the article "security and privacy issues in e-passports" from Juels et al., 2005, the privacy and security implications of the introduction of RFID-chips and biometrics in passports is examined. The main points raised in this study are: clandestine scanning; clandestine tracking; skimming; cloning; eavesdropping; biometric data leakage; and cryptographic weaknesses.

Clandestine scanning

Clandestine scanning means that e-passports can be scanned illegally/secretly. This is because no authenticated or encrypted communication between passports and readers is required. As a result, the chips can be subjected to clandestine scans at short distances (up to a few meters), where sensitive information such as a person's date of birth and place of birth can be leaked (Juels et al., 2005). Encryption refers to the process of converting readable information into coded information (Enahoro, 2019). This encrypted information is often presented as ciphertext and ensures that third parties (unauthorized persons) cannot decipher the information (Ehrsam et al., 1978).

Clandestine tracking

Clandestine tracking means that passports can be traced. This is possible because the data on the chip can also be read without authentication (Juels et al., 2005). Multiple clandestine scans can lead to clandestine tracking because the RFID technology offers the possibility to track a person's movements. A person can be tracked by the biometric information released during the scanning of the RFID chip (Lekkas, 2007).

Skimming

Skimming means that the information on a chip can be read secretly. An RFID reader that is installed in a door frame will have a large enough range to be able to read the chips, (the range is around 90 cm). Then the data of everyone with an RFID chip implemented in their passport can be read when they pass the doorway. These RFID readers can be installed as part of airport

security checkpoints, sporting events or concerts, but in theory could also just be placed in shops or building entrances. These readers can look a lot like the anti-theft gates that are already used in thousands of shops, so that passport holders will not think their data is being skimmed (Juels et al., 2005).

Cloning

Cloning is copying or duplicating the data on a chip to another chip or system (Bogari et al., 2012). Several researchers conclude that cloning is a serious vulnerability of e-passports. Lukas Grunwald, CTO of German security consultancy DN-Systems Enterprise Internet Solutions, stated during a presentation on RFID technologies that the first generation of passports designed using the ICAO standard can be easily cloned (leyden, 2006). The article from Juels et al. claims that cloning can happen despite a digital signature is being required on e-passport data. This signature helps the reader to verify that the data on the passport is from the correct passport issuing authority. However, this signature does not bind the data to a specific RFID chip and therefore not to a specific passport. Passports can therefore easily be cloned (Juels et al., 2005).

Eavesdropping

Eavesdropping is the biggest security problem in RFID systems (Weis, 2007). Eavesdropping, is possible because passports are not only displayed at airports, but also, for example, when checking in at a hotel or picking up a postal package. Providers of these services can then easily access the data on the RFID chip of a passport, even though they may have wrong intentions (Juels et al., 2005).

In the Netherlands, a copy of Identity Documents is often requested, for example when taking out a telephone subscription. In principle, this should not be required, but there are exceptions. Some parties are allowed to make a copy of identification documents or overwrite certain data. The organizations that are authorized for this are: government agencies, banks, notaries, casinos, life insurers, and employers (Rijksoverheid, n.d.)

Biometric data leakage

Biometric data leakage is linked to the biometric images contained in e-passports. These include fingerprints, passport photos in colour and images of the iris of the eye. This information has been added to the passport because it is sometimes difficult for humans to distinguish between people on the basis of a black and white photo. Computers could do this better using biometrics. An additional danger is that this important information could leak (Juels et al., 2005).

Cryptographic weakness

Cryptographic weakness is linked to the authentication and encryption mechanism guidelines for passport-to-reader communications set up by the ICAO. This mechanism ensures that the chip in the passport itself can determine that it is going to release information to a legitimate reader. However, this access will never expire if it is provided to a reader. This means that a passport holder traveling abroad gives that country's customs agents the ability to scan his or her passport forever (Juels et al., 2005). According to Ehrsam et al. cryptography is the only known technologically feasible method to protect stored data. In his study on cryptographic key management, he defines cryptography as methods or writings that are intended to be incomprehensible to anyone except those who legitimately have the means to recover the original information. Cryptography can be used to protect data from the threat of eavesdropping and theft (Ehrsam et al., 1978). He adds that the challenge in cryptography is coming up with a secure method that converts messages as plaintext into cryptograms (Ehrsam et al., 1978).

Other sources, acknowledge those points as threats for e-passports. In the article “no encryption for e-passports’, it is mentioned that the lack of encryption amazed privacy advocates and security researchers. They say the new passports are vulnerable to “skimming” (Singel, 2005). The author also states that the State Department has admitted that skimming is a legitimate threat. However, the Ministry also claims that the chips will have a reading range of inches so that eavesdropping at border stations would be very noticeable and that the passports will have a shielding mechanism. This could be, for example, tissue in the passport cover that protects the chip when the passport is closed (Singel, 2005). In an article from Ramya et al., this cover is described as “the faraday cage”. This is a much-discussed countermeasure against clandestine RFID scanning. In an e-passport, a faraday cage would take the form of metallic material in the cover or holder that prevents the penetration of RFID signals. Passports fitted with faraday cages would only be scanned if expressly shown by their holders (Ramya et al., 2018)

According to Neville Pattinson, during the early development of e-passports, it was discovered that the RFID chip in a passport could be read by intercepting radio signals between passports and passport readers at a distance of up to ten meters. He also claimed that this was an obvious issue that required additional security measures to preserve citizens' personal privacy and national security. On the other hand, Pattinson (2021) adds that this issue was addressed by governments at the time and special technologies were developed to ensure that passport chips only communicate with authorized readers (Pattinson, 2021).

After explaining the various risks associated with the implementation of an RFID chip, the article RFID security threat model written by Thompson et al. discusses the consequences that can arise if a person's data is leaked. Identity theft, tracking and hot listing are described as problems that arise from leakage of e-passport data which extent beyond the e-passport system itself. A criminal can build a new identity or create a fake document with a photo, name, date of birth and social security number. In addition, identification makes it possible to track the movements of the RFID chip from the passport. Combined with other information, this could provide insight into a particular person's habits. Hot listing is the most dangerous consequence of data leakage because it explicitly allows targeting specific individuals. An unpleasant prospect is an 'RFID-enabled bomb', an explosive device designed to explode upon the RFID reading of a particular person (Xiao et al., 2009). The chip in an individual's passport contains information about the passport holder's nationality. When this information is exposed to an unauthorized user, this is a huge threat because for example a bomb in a restaurant can explode when there are five or more people with a specific nationality physically present in this place, or a smart bomb positioned at a street corner explodes when a particular person with an e-passport is detected (Thompson et al., 2006).

Identity Theft

According to Ronald Leenes, 'identity theft' is rarely defined in a precise and clear way. He states that much of the literature provides descriptions or working definitions (R. Leenes, 2006). This corresponds to the statement from Katrine Baum from the U.S. Department of Justice. She stated that there is no universally accepted definition of identity theft, and that the concept describes a variety of illegal acts related to theft or misuse of personal information (Baum, 2006). According to Sven Geenens, the Dutch government also does not know exactly what the concept of identity theft means. This is evident, for example, from a response from the Minister of Justice, who defined identity theft as any type of crime consisting of fraudulently obtaining and using the identity of another person with the intent to commit fraud or carry out other criminal activities (Geenens, 2014).

Tracking

Tracking is a broad concept which different meanings. Lauri Oksama and Jukka Hyona published a study on position tracking and identity tracking. In this study, identity tracking is defined as connecting identities to their locations (Hyona, 2016).

Hotlisting

A hotlist is as a set of identities that respect a given property. Hotlisting is the ability to determine if an identity belongs to a certain hotlist (Bocchetti, 2006). The ICAO did establish a large number of guidelines to ensure the authenticity and privacy of the data on the RFID chip. These guidelines contain a range of cryptographic measures including passive authentication. This means that the data stored on an e-passport is signed by the issuing authority, which ensures that the data is authentic (ICAO, n.d.). However, the problem with this is that this measure only ensures that the data on the chip is authentic, but not that the passport around the chip is authentic. The ICAO guidelines also specify two optional cryptographic features for enhanced security in e-passports. Those features are active authentication and Basic Access Control (BAC).

Active authentication

Active authentication focusses on preventing unauthorized parties from reading the contents of e-passports. This feature is based on cryptography and allows the reader to distinguish the authenticity of a chip from a counterfeit (Juels et al., 2005). Active authentication is also known as an anti-cloning mechanism. This cryptographic feature is not mandatory according to ICAO guidelines, but the EU specifications about e-passports do require its use (Bogari et al., 2012).

Active authentication increases the cryptographic capabilities of a chip. This is an advantage over passive authentication because with active authentication, the same key pair is always used for an authentication session, instead of the temporary keys used during passive authentication (Bogari et al., 2012).

Basic Access Control

BAC is one of two optional security features specified in the ICAO standard for first generation e-passports. So, BAC is optional in the ICAO standard and not mandatory. However, the EU specifications for e-passports do require the use of BAC for EU countries for enhanced data protection (Bogari et al., 2012). BAC is a measure that ensures that tag data can only be read by authorized RFID readers. This is possible because BAC stores a few secret cryptographic keys in the passport chip. When a reader tries to scan the passport, it switches to a challenge-response protocol that demonstrates knowledge of the key pair. If authentication is successful, the passport will release its data content, otherwise the reader will be considered unauthorized, and the passport will deny read access. Neville Pattinson, advocated for BAC in his previously described paper (Pattinson, 2004). Additionally, Bart Jacobs, a Dutch scientist and professor of

security, privacy and identity at Radboud University, also emphasizes in his paper "Biometry in passports" the importance of BAC (Jacobs, 2005).

However, BAC also has drawbacks. There is a way to find out the key of the passport chip if one knows the passport number, date of birth and expiry date of the passport. This data, together with some check digits, form the access key, which in theory could easily be cracked by hackers (Bogari et al., 2012).

Jaap-Henk Hoepman discusses the issues surrounding security and privacy of e-passports in his article "Crossing borders; security, and privacy issues of the European e-passport". Contrary to the articles referred to earlier, BAC is not seen here as a solution to improve security but is attacked because of the low entropy of the data from which the access keys are derived (Hoepman et al., 2008).

The authors of the article "security and privacy issues in e-passports" concluded that the unauthorized reading of e-passport data poses both a security and privacy risk. According to them, this risk will only increase because of the uncontrolled use of biometric identification. Therefore, the authors argue for ICAO regulations stating that at least the Faraday Cage and BAC must be used to prevent unauthorized reading of e-passports remotely.

Identity Fraud

Now, we understand more about the safety and security risks associated with the implementation of RFID chips in passports. To better understand the impact of the implementation of biometrics on passports to combat identity fraud, the article "Biometrics and identity fraud protection: two barriers to realizing the benefits of biometrics – a chain perspective on biometrics and identity fraud" from Jan Grijpink creates clarity. It examines which barriers still need to be overcome in order to be able to use the advantages of biometrics against identity fraud.

Identity fraud is the key concept of this research and is defined as the act of intentionally impersonating an identity that does not belong to this person by using another person's identity or a fictitious identity (Grijpink, 2005). A more specific type of identity fraud is look- alike fraud. Look- alike fraud could be defined as the use of a passport by somebody who resembles the rightful owner (Grijpink , 2004) . According to Jan Grijpink, identity fraud is often the first

step to the next stage of fraud, such as bank fraud, passport fraud or benefit fraud. Jan Grijpink also wrote the article "Identity fraud as a challenge to the constitutional state", in this study, published in 2004, he stated that the methods of identity verification at the time had to change to counter the challenge of identity fraud in the future because existing identity policies were no match for guaranteeing security and privacy in an information society (Grijpink , 2004).

Categories of Identity Fraud

Identity fraud committed with documents can be committed in various ways. The ECID distinguishes three categories; a document can be false, forged, or authentic (Royal Dutch Marechaussee, 2020).

- A false document is a completely counterfeit (existing) document. This is also known as a reproduction.

- A counterfeit document is a good (authentic) document to which unlawful adjustments, additions or deletions have been made.

- An authentic/good document is a technically approved document. However, identity/document fraud can be committed with a technically approved document. This may be because there is no resemblance between the owner and the user (also called lookalike or imposter), or the document may have been obtained fraudulently (Royal Dutch Marechaussee, 2020).

Jan Grijpink claims that in general it appears that measures and instruments that are useful for combating document fraud do not offer solutions for combating identity fraud and often even have the opposite effect. The example given here is the Dutch measure from 1996 in which listing a citizens' service number on the Dutch passport was introduced. This measure has led to an enormous and growing amount of identity theft. This is because this name-number verification is only effective if the identity document meets all requirements, and the holder is the right person. However, this is no longer the case if it is used by someone else who looks like the official document owner (Grijpink, 2005).

Listing the social security number on identity documents has therefore unintentionally made identity fraud much easier. From this it is concluded that this is also an obvious consequence

after the implementation of a biometric detail in identity documents. If an identity fraudster can figure out what metric or image their biometrics are being compared to, there are many deceptive ways to trick the automatic identity checker (Grijpink, 2005).

Victor Lee claims that biometric technologies are a promising tool in the fight against identity theft. Conditioned that they are used carefully and considering the capabilities and vulnerabilities of the technology and the potential and likely impact it has on society (Lee, 2008). In the article "Biometrics and identity fraud" he investigates the link between biometrics and identity fraud. The article provides clarity on how biometric technologies improve alternative identification and authentication technologies, how the biometric systems themselves can be targeted by identity fraudsters, and finally, it discusses societal and operational challenges arising from the use of biometrics in the fight against identity fraud.

Biometrics

Biometrics is an important concept of this study and could be defined as the science of establishing a person's identity based on a person's physical, chemical, or behavioural characteristics (Jain et al. , 2008). According to Egon van den Broek, the focus on biometrics has fluctuated in recent decades and in this century the focus on biometrics has been strengthened by the need for large-scale identity management systems. He also states that biometrics can be used to verify a person's identity by comparing captured biometric data of a person with that person's biometric data stored in a database. (Broek, 2010). Biometric authentication is the process of authenticating individuals on computers using biological or physiological characteristics (Nithyanand, 2009).

The biometric authentication procedure for e-passports involves two processes, which are registration and verification. Registration is the process by which the e-passport applicant registers their biometric data in a secure location under human supervision. Subsequently, these biometric data are encoded, after which they are stored on the RFID chip of the passport applicant. The second process in biometric authentication is the provision of biometric data by the user for identity verification. The supplied data is compared by an algorithm with the registered data. If they match, the biometrics are accepted and the identity verified (Nithyanand, 2009).

Human Identification Theory

This process of registration and authentication for identification fits within the developed theory of Roger Clarke (1994). This theory is named “the human identification theory” and holds that all human identification fits a single model. This model includes the process of association of existing data of a particular person with the data supplied at that time. This process starts with the registration of characteristics of a person. When this individual subsequently wants to interact with the identifier, an identity document must be presented that can be checked with the data provided (Clarke, 1994). During the identification process, the identifier is trying to match the characteristics of a person observed in a first observation with the characteristics of a person observed in a second observation to determine whether they are the same person (LoPucki, 2001). Clarke defined human identification as the association of data with a particular human being (Clarke, 1994). Additionally, he identified three basic means for making human identifications. Those means are knowledge-based identifications, token-based identifications, and biometric identifications.

"Knowledge-based" identifications identify a person by demonstrating that they possess information that only that person should know. Examples are bank account number, social security number, passwords, mother's maiden name, and drivers license number.

"Token-based" identification identifies a person by possessing a specific item such as a passport or driver's license. Such an item is called a token and contains characteristics of the person to be identified with it. This way provides extra security compared to knowledge-based identification because a fraudster may not use the token because the personal characteristics in the token do not match those of the fraudster.

Biometrics have several advantages. For example, this technology ensures that people no longer have to remember their passwords or PINs, because they can prove in another way that they are authorized to gain access. People often choose easy passwords that can be guessed or hacked, they do this because they are afraid that they will forget difficult passwords. Biometrics removes this disadvantage because those characteristics are distinctive and personal. The transfer of this data from one individual to another is very tedious which leads to a decrease in phishing attacks which reduces fraud (Lee, 2008).

Another advantage of using biometrics is efficiency. The constantly increasing flow of passengers at airports means that queues are getting longer. While attracting more staff is often not an option due to costs, these large numbers of passengers must still be guided through the airport process in a safe and pleasant way. Failure to do so will lead to chaotic situations and dissatisfied travellers. This comes at the expense of both safety and the quality of the travel experience. Both pose a threat to the business of an airport or airline. In intensive and complex passenger movements, biometrics can provide greater efficiency, while it improves the level of security and ease of use at the same time (Snijder, 2010). An e-Gate is an automatic self-service border control where the traveller scans the passport himself to cross the border. Persons older than 16 years with an EU passport with a chip can pass the automatic passport scanners. The e-Gates work with biometrics and the photo the e-Gate takes of a face is only used for border control and deleted after 24 hours (Coosemans, 2020).

Besides advantages, biometrics also have disadvantages. For example, the implementation of the technology is very expensive, and invasion of privacy is lurking (Babich, 2012). In addition, according to Roger Clarke, a problem he describes as ‘the entry-point paradox’ can arise. He argues that the identity to which the characteristics are attributed may still be 'false'. For example, a finger can be separated from the body, or a criminal can still relatively easily obtain biometric data from others and use it fraudulently. An additional problem is that as long as no criminal has been arrested walking around with your biometric data, it is very difficult to prove that it was not you. In short, the consequences of biometric fraud are very serious and much difficult to recover (Derksen, 2009).

Public Key Infrastructures

The latest technology in e-passports is Public Key Infrastructures (PKI). This technology is used to authenticate the data stored electronically in the RFID chip. This makes it difficult and expensive to counterfeit the chips. PKI consists of several elements, but the security mechanism is broadly about the key pair of the RFID chip. This key pair must be generated by the issuing country and stored in a highly secured infrastructure. Each participating country is responsible for downloading the latest version of the keys and for ensuring that the passports are indeed signed by the document signer (Kundra et al., 2014).

Passport Generations

To date, the ICAO and the EU introduced three generations of e-passports. The first two of those generations are being issued worldwide (Bogari et al., 2012). The ICAO described three cryptographic technologies in the specifications for the first-generation e-passports. Those technologies in e-passports are biometrics, PKI and RFID. Since the introduction of the first generation of passports, several security vulnerabilities have arisen. Eyad Abdullah Bogari of the Concordia university college of Alberta and his colleagues have published an analysis of security weaknesses in the evolution of RFID enabled passport. This document presents the evolution of the different generations of e-passports through the years in order to find a correlation between the weaknesses (Bogari et al., 2012). Rishab Nithyanand from the Stony Brook University in New York published a similar study on the evolution of cryptographic protocols in e-passports (Nithyanand, 2009). Both studies clearly describe the changes in e-passport guidelines over the years.

First generation

The guidelines for the first generation of e-passports were drawn up in 2004. They stated that it was mandatory to put a photo of the face of the passport holder on the chip. Adding other biometrics was not mandatory but allowed (examples are fingerprints and iris images). Three cryptographic protocols are described in the ICAO first-generation e-passport specifications to ensure data accuracy and privacy. These are passive Authentication, Basic Access Control and Active Authentication (Nithyanand, 2009).

Second generation

In 2006, the ICAO presented a new set of guidelines for e-passports. The second generation of e-passports was implemented to address the weaknesses of the first generation (Bogari et al., 2012). The biggest change in the guidelines was the addition of Extended Access Control (EAC). The goal of EAC was to provide more comprehensive tag and reader authentication protocols and to ease the implementation of secondary biometrics for added security (Nithyanand, 2009). The addition of extra biometric features such as fingerprints was necessary for security and access controls at the border (Bogari et al., 2012). To achieve mutual authentication, the EAC proposal introduced two new protocols called Chip Authentication and Terminal Authentication. These were used in addition to the Passive Authentication protocol, the Basic Access Control protocol, and the Active Authentication protocol described in the first-generation e-passport specifications (Nithyanand, 2009).

Third generation

At the end of 2008, the Federal Office for Information Security released a document which described new security mechanisms for e-passports. The third generation of e-passport guidelines introduced a new technology called Password Authenticated Connection Establishment (PACE). In addition to PACE, the second-generation Terminal Authentication and Chip Authentication protocols were also updated. The PACE protocol was introduced as a replacement for the Basic Access Control mechanism. PACE is a mechanism that enables an RFID tag to verify that a reader has authorized access to the electronic passport, this is possible because the tag and reader share a common password (Nithyanand, 2009). PACE allows the verification mechanism to have more control over the e-passport by preventing the chip in the passport from allowing access to the data stored on the passport if the distance at which the passport is scanned is too big (Suhaimi et al., 2020).

The existing literature provides a lot of clarity about the advantages and disadvantages of e-passports and biometrics. The security and privacy issues and possible solutions for additional security measures are discussed in detail. However, there is a gap in the literature. Much research has been done on the pros and cons of e-passports and in particular their safety and security, however the literature does not elaborate on the magnitude of the impact of e-passports on identity fraud. This phenomenon is actually still unexplored, and little is known about the impact that the chip with biometric data in passports has had on identity fraud, especially look alike fraud.

With the knowledge from the analysed academic articles from the literature review, two hypotheses can be developed regarding the impact of the introduction of e-passports on identity fraud. The addition of biometric data on the chip, made it more difficult for fraudsters to impersonate someone else because more external characteristics are checked. Therefore, it could be stated that the implementation of RFID-chips on passports caused a decrease in look-alike fraud. Additionally, due to the digitization of the identification document, the fraud will also digitize. Where previously fake passports were made and used at, for example, a border control or the counter of a bank office for applying for an account, a chip will now be hacked to adjust or delete the data. Therefore, it could also be stated that the implementation of RFID-chips in passports has caused a shift in the way identity fraud is committed.

Summarized Table Most Important Concepts

Concept	**Definition**
E-passport	A passport in which an RFID tag with relevant biometric information of the owner is implemented is called an electronic passport or e-passport (Nithyanand, 2009)
Identification	Identification is establishing someone's identity to verify that someone is actually who they say they are (Brummelkamp, 2020).
Identity	People's concept of who they are, of what sort of people they are, and how they relate to others" (Hogg & Abrahams, 1988, p. 2)
Identity theft	Any type of crime consisting of fraudulently obtaining and using the identity of another person with the intent to commit fraud or carry out other criminal activities (Geenens, 2014).
Identity fraud	The act of intentionally impersonating an identity that does not belong to this person by using another person's identity or a fictitious identity (Grijpink, 2005).
Look-alike fraud	Look- alike fraud could be defined the use of a passport by somebody who resembles the rightful owner (Grijpink , 2004)
RFID	Radio-Frequency Identification (RFID) technology is a wireless sensor technology based on the detection of electromagnetic signals (Domdouzes et al., 2007)
Biometrics	The science of establishing a person's identity based on a person's physical, chemical, or behavioural characteristics (Jain et al. , 2008)
Basic Access Control	BAC is a measure that ensures that tag data can only be read by authorized RFID readers
Biometric authentication	Biometric authentication is the process of authenticating individuals on computers using biological or physiological characteristics (Nithyanand, 2009).
Personal Identity	The uniqueness of an individual that emerges on the basis of identity tags (name, biometric features, characteristics) and the individual biography (Müller, 2008).

Methodology

This section will explain the methods used to test the developed hypotheses and answer the main and sub questions of the study. In addition, the limitations of the research with regard to reliability and credibility will be explained.

Research design

For this research, the results and conclusion are based on statistical data. This means that the study is quantitative.

Data collection methods

To answer the research question, desk research, literature research and field research were used. Desk research was carried out in the form of database studies, the analysis of reports and the analysis of numbers. Field research was conducted in the form of interviews.

Desk research

The Expertise Center for Identity Fraud and Documents (ECID) is the national contact point for identity fraud and documents in the Netherlands. This organization is a partnership between the Royal Netherlands Marechaussee and the police. The center provides advice and information on preventing and combating identity and document fraud. As a result, the ECID makes an important contribution to combating identity fraud in the Netherlands (Koninklijke Marechaussee, 2015). This research used the the statistical annual overviews in which figures on document fraud are published.

Additionally, the data from the “monitor identity” is analysed. The “monitor identity” has been in existence since 2014 and it is used every two years to keep track of how often, in which situations and in what way people identify themselves. It also shows how often this goes wrong and people become victims of abuse of their identity data (Brummelkamp, 2020) (Brummelkamp, 2020). The monitor contains figures in the field of identities, identity fraud and identity management for both the public and the private domain. This made the publication the first of its kind, and therefore the information from the document was used to provide insight into the starting points for policy (Ministerie van Binnenlandse Zaken en Koninklijksrelaties, 2013).

In addition, a government report was analysed. The Ministry of the Interior and Kingdom Relations published the report "Identity in figures" on December 12, 2013. This government report is based on the monitor identity and contains findings and interpretations about the first editions of the monitor (Ministerie van Binnenlandse Zaken en Koninklijksrelaties, 2013).

Field research

In order to get a good picture of the figures of identity fraud and the way in which fraud is committed, the vision of an expert in this field is important. That is why I interviewed two employees from the ECID. In this way I could also ask specific questions about the publications of identity figures and the possible underlying causes and consequences.

Data characteristics

This study focuses on the impact of the implementation of an RFID chip in passports on identity fraud in the Netherlands. The European Union (EU) has complied with implementing the chip in August 2006 and the Netherlands implemented the measure on already June 28th that year. Because no clear cut-off is detectable (not everyone with a Dutch passport had to have their non-RFID passport surrendered and replaced by this date), the results will be analysed using time periods.

The fraud data is analysed over three different time periods and then compared to each other to draw conclusions.

1. Period before the 28th of June 2006 (when the chip was not yet implemented). However, only data availability from 2004. So, 2004, 2005 and 2006 will be the 'pre implementation period'.
2. Period 2007-2016 (a passport is valid for 10 years in the Netherlands).
3. Period 2017-2021 (period in which all passports are equipped with the RFID chip).

Limitations

A limitation of this research is the availability and accessibility of data. The ECID whose data will be used has only been in existence since 2008 and in addition there is a data retention period so numbers related to identity fraud may be difficult to trace.

Data Sources

To answer the central question of this research, different data sources were used. These are the: European monitor identity, the National Office for Identity), the identity fraud and documents centre of expertise, and the Dutch Central Agency for statistics. In this chapter these public organizations will be described.

European Monitor Identity

Since 2013, the Ministry of the Interior and Kingdom Relations has been carrying out the Monitor Identity. Every two years, this monitor keeps track of how often, in which situations, and in which way citizens identify themselves in the Netherlands and how the government guarantees its quality. It also shows how often this goes wrong and people become victims of misuse of their identity data. The aim of the Monitor Identity is to provide insight into the identification traffic between citizens, companies and governments. The results of the monitor are used to help the House of Representatives to make policy choices. The results of the monitor are published every two years, which ensures that the status quo, historical developments and changes are made clear. The monitor thus provides an overview of the development of identity verification over the years, making it clear how physical identity verification is shifting to digital identity verification and how forms of abuse develop and possibly shift (Panteia, 2015).

National Office for Identity Data (RvIG)

The National Office for Identity Data manages the Dutch basic register of persons, is responsible for the technical systems for the storage and exchange of personal data, issues citizen service numbers and manages the travel documents of the Kingdom of the Netherlands. The National Office for Identity itself claims that innovation is playing an increasingly central role in the field of identification. That is why the National Office for Identity is developing new software for travel documents and is improving the application and issuance process. They are also involved in the development of e-passports, with which citizens can also identify themselves online (National Office for Identity, 2020). This organization was contacted with the question whether they could provide data on the number of Dutch passports and identity cards issued and in circulation in a particular year.

Identity Fraud and Document Centre of Expertise (EICD)

The ECID is a partnership between the Royal Netherlands Marechaussee (KMar) and the National Police (NP). The center provides advice and information on preventing and combating identity and document fraud. The ECID mainly works for the Royal Netherlands Marechaussee, the police and the Public Prosecution Service. But also, for the Ministries of the Interior and Kingdom Relations, Foreign Affairs and Justice and Security, national and international enforcement and investigative services and partners that work in the so-called identity chain. These are bodies that successively deal with establishing, recording and checking an identity or proof of identity. The KMar is an important part of the EICD, the activities of the KMar include many border security tasks, which means that this organization has special expertise in the field of identity determination and identity fraud, in particular in the field of travel, residence and/or identity documents. The main task of the KMar is to examine documents, to establish their authenticity, to draw up the technical report regarding these documents and in some cases to further handle the (criminal) investigation. In addition, they make an important contribution to the information provision of the ECID and information and technical support is provided to chain parties such as the NP, Customs and municipalities. Through its expertise and active collaboration with partners, the ECID makes an important contribution to an effective approach to identity fraud in the Netherlands (Royal Dutch Marechaussee, 2020).

Dutch Central Agency for Statistics (CBS)

The Dutch Central Agency for Statistics was founded in 1899 and produces and publishes static information about Dutch society. The CBS publishes data in many different areas for the benefit of government, science and society. The CBS database contains static data on population composition, population growth, economic growth, unemployment, crime and much more (Rijksoverheid, 2020).

Statistical Annual Reports Identity Fraud and Document Centre of Expertise

The statistical reports of the EICD will be analysed and the useful data will be used to answer the main and sub-questions. The reports contain an enormous amount of information about document fraud, but only the chapters on Dutch document fraud will be used. The statistics with data on identity fraud with foreign documents cannot be used because the graphs and tables do not indicate from which country the documents originate. It is therefore also impossible to

find out whether the documents are within or outside the EU, which makes it impossible to determine whether the documents were issued in a country where RFID chips with biometric data are used. This research is also generally limited to the Netherlands because it is clear when the RFID chips are made mandatory in this country and because the data available is mainly focused on Dutch identification documents.

Document fraud encompasses not only the concept of passport fraud, but also identity fraud involving other documents, including driver's licenses and identity cards. The table “Types of document fraud” was used to determine what percentage of document fraud in the Netherlands in the year in question consisted of passport fraud. This made it possible to determine what percentage of the total fraud was accounted for by passport fraud.

The table with data on the modus operandi of Dutch passports was used from each annual report to determine the form in which fraud was committed with Dutch passports in that year. This can vary from look-alike fraud to, for example, falsifying personal data.

Interview

To better understand the data from the ECID's annual reports and to ask for possible explanations of the data to draw the correct conclusions, an interview took place. The interview took place with Mrs. Lonneke Bontje and Mr. Alexander Castanon. Mrs. Bontje is head of the analysis bureau and senior analyst at the ECID. Mr. Castanon works in the Advice & Development department, where he is also the head of the bureau.

Data Explanation

Through a Wob-request, the official statistics on lookalike fraud involving Dutch passports and identity cards were made public for the first time. If the available (government) channels do not provide sufficient information, a request can be made to disclose government information. This is called a Wob request. Anyone can request the government for information about an administrative matter. Non-Dutch citizens can also submit a Wob request to the Dutch government. Information provided by means of a Wob request is immediately made public to everyone in accordance with the Disclosure of Government Act (Wob). The annual reports of the EICD contain the necessary data for this research. The main definitions from the tables and graphs will now be briefly explained to clarify the statistical data.

The annual reports contain various forms of fraud that can be committed with documents. Document fraud is divided into three types: false documents, forged documents and good (authentic) documents. A definition will be given for each of these categories and the various associated modus operandi will be described.

Fake document

A false document is a completely counterfeit (existing) document. Also called reproduction.

Modus Operandi:

- Totally false

Totally false:

Full reproduction of an existing passport

Counterfeit document

A forged document is a good (authentic) document to which adjustments, additions or deletions have been made. This falsification of a document can be done in a number of ways.

Modus operandi:

- Personal details page false
- Personal details page forged
- Replace Personal Details Page
- Page removed (other than personal details page)
- Blank stolen
- False stamp(s)
- Replace Photo
- Variable data falsified
- Damaged/destroyed
- Visa forged
- Other counterfeits

Blank stolen

Authentic documents are sometimes stolen blank. This is reported by the authorities. The theft takes place before the documents are registered. The filling in is therefore done by the forger and as a result the document is forged.

Variable data falsified

Changes to variable data that are not part of personal data, for example MRZ codes and issue details.

Personal details page false

This modus operandi includes the so-called 'sticker method'. This method involves applying a (partially) printed foil over the physical personal details page of an identification document. In this way, the originally applied personal data and the photo can be masked. There are often no security features in the foil and the document can easily be recognized as forged during a physical check.

Good / Authentic document

A technically good, authentic, document used by another, or a good document obtained on false (fraudulent) grounds.

Modus operandi:

- No resemblance ("look-alike", "impostor")
- Stolen/missing
- Fraudulently obtained
- Fantasy

No resemblance ('look-alike', 'impostor')

In a case of no resemblance, there is usually nothing wrong with the document. The person using the document is not the rightful owner. The person with the document thus pretends to be someone else to achieve something, often this is done to be able to cross national borders. This form of fraud can only be determined if there is sufficient discrepancy between the suspect and the photo provided in the document or if the suspect's fingerprints do not match the fingerprints stored in the document.

Stolen/missing

By reporting the loss or theft of a (travel) document, it loses its validity. By still traveling with this one is committing a criminal offence. If someone else uses this document and is arrested, the case will be registered under the Modus operandi, no resemblance to the statement that the document was registered as stolen/missing.

Fraudulently obtained

Documents are found that were issued after presenting a false or forged document. The documents are therefore technically good but obtained on false grounds.

FSD Schiphol, Helpdesk Schiphol, and the other counterfeit desks

The ECID's annual reports contain statistics from the Schiphol Counterfeits Desk (FSD), the Helpdesk at Schiphol and the counterfeit desks with a similar helpdesk function in the three other regions of the Royal Netherlands Marechaussee (South, North-East and West).

The FSD handles cross-border cases originating from Schiphol Airport. If doubts arise about the authenticity of a document during a check at Schiphol, the document is presented to staff of the FSD. If there is any doubt about the identity of the user of the document, the user will also be taken to the FSD.

The ECID has a counterfeit desk in every region where the Royal Netherlands Marechaussee operates. This is where matters are handled that are found in the country during border controls by Marechaussee, for example during mobile surveillance and security (MTV) controls. If an employee of the Marechaussee who carries out the check is in doubt about the authenticity of a document, the document can be presented to one of the desks. The cases of document fraud involving border crossings (outside Schiphol) from the reports were therefore presented to a counterfeits desk. Those desks also handle cases of document fraud that are found during activities that do not involve border crossings, for example from traffic checks by the Marechaussee or during investigations into human trafficking or people smuggling. The counterfeit desks serve as a point of contact for questions about documents and means of payment. Not only for the Marechaussee, but also for other public and private organizations.

The Helpdesk at Schiphol is most often used as a point of contact for questions about documents. The documents can be presented physically, but also in faxed or e-mailed form.

Results

The following pages will present the analysed results. The legend below indicated the different time periods.

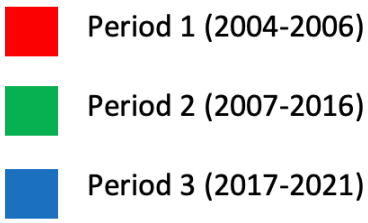

Figure 1, Legend

Number of cases/suspected persons FSD Schiphol desk

First, the number of cases at the FSD Schiphol desk. These are all suspected persons who were taken to the FSD desk at Schiphol for inspection because there was doubt about their identity. The ECID reports contain Figures from 2001 to 2020. The three different time periods are shown in colour for clarity, the legend can be found in Figure 1.

As can be seen in the table and the accompanying graph, there has been a clear decrease in the number of cases at the FSD Schiphol Desk over the years. There are some outliers, especially in the last period. The average number of cases in the first period is 2298, in the second period this number is 748 and in the last period 836. So, a very clear decrease is noticeable from period one to two, but a slight increase in the last period.

Year	Cases
2001	2660
2002	2765
2003	2564
2004	2361
2005	1910
2006	1530
2007	1137
2008	951
2009	644
2010	660
2011	815
2012	578
2013	626
2014	729
2015	598
2016	740
2017	843
2018	690
2019	896
2020	916

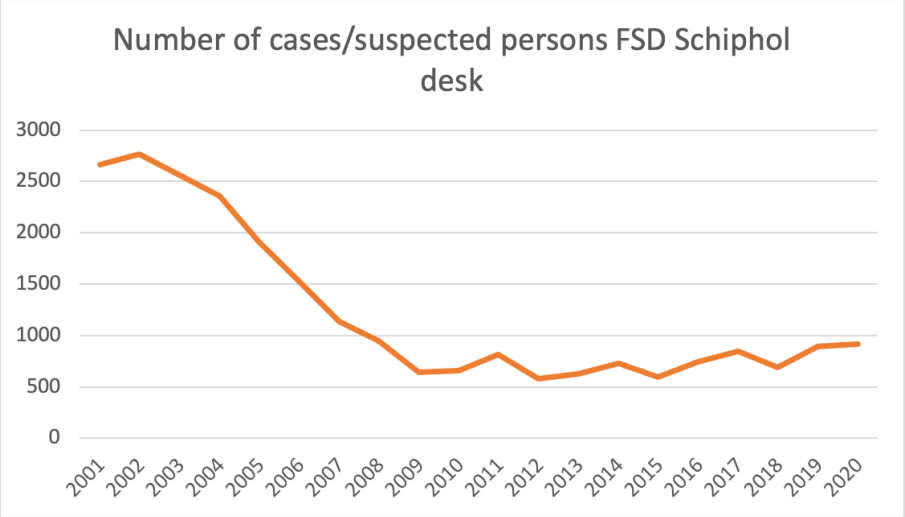

Figure 2, Cases FSD Schiphol Desk

Fraudulent Documents

The table and graph below show the figures for the number of documents presented for verification and the number of them with which fraud has been committed. The last column of the table shows the percentage of documents with which fraud was committed compared to the total number of documents presented for verification. From this it can be concluded that this number is in a downward trend from 2004 to 2013. From the end of time period two to time period three, the downward trend is less clearly visible and the number of documents with which fraud has been committed increases in both absolute and percentage terms.

Year	Number of documents presented for verification	Number of documents with which fraud was committed	% Of documents with which fraud was committed compared to the total number of documents presented for verification
2004	28391	2840	10
2005	26209	2358	9,0
2006	21935	1886	8,6
2007	17936	1434	8,0
2008	19796	1334	6,7
2009	27366	882	3,2
2010	36416	979	2,7
2011	47522	1137	2,4
2012	33307	806	2,4
2013	31838	854	2,7
2014	24565	1158	4,7
2015	34650	1100	3,2
2016	32130	945	3,4
2017	41952	1104	3,8
2018	43696	1181	3,7
2019	30987	1223	3,9
2020	29874	1019	3,4

In Figure three, the wave pattern is showing that the number of documents presented to the FSD for verification is not in a clear decreasing or increasing trend. In Figure four is the total number of documents with which the FSD has established that fraud has been committed, presented in a line graph. It can be seen here that this line was in a sharp downward trend until about 2009 and that the number has stabilized after that and continues in a wave motion. Time period one together with the beginning of time period two is thus the period when the number of documents

was in the decreasing trend. Thus, no clear change in the trend is visible from the chip's implementation period, as the downward trend is already visible in period one.

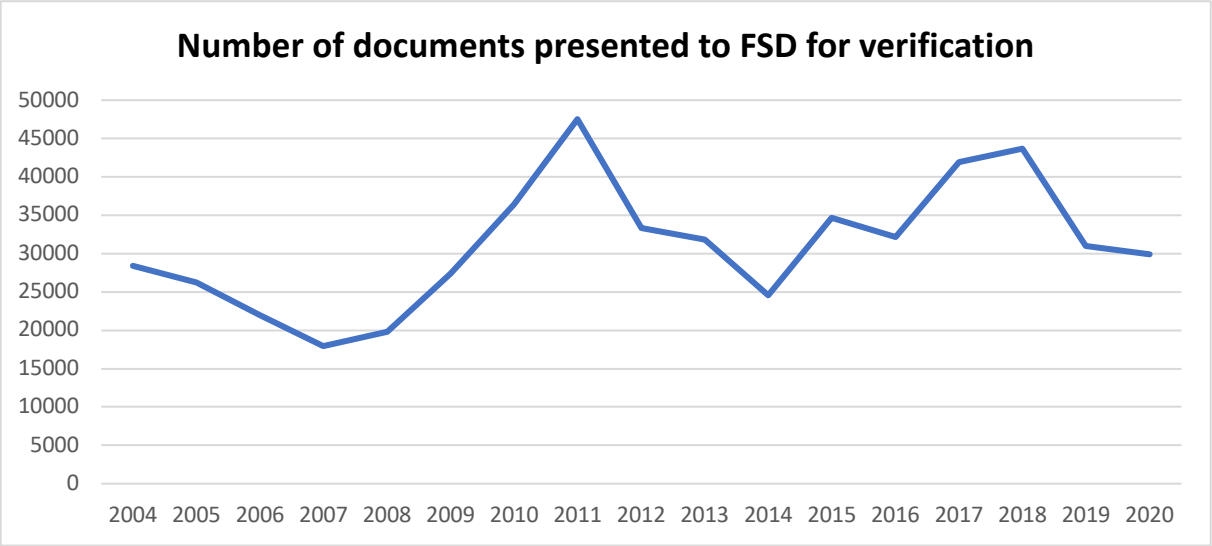

Figure 3, Number of documents presented to FSD for verification

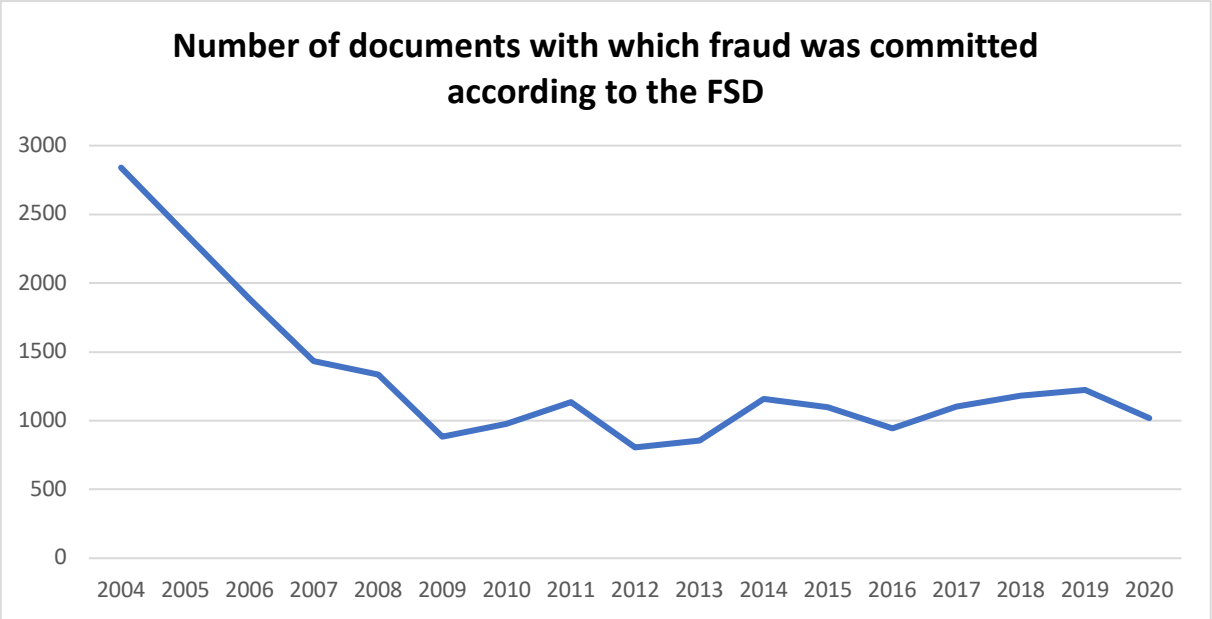

Figure 4, Number of Documents with which fraud was committed

Share of the type of document with which fraud was committed

The total number of documents with which it has been established that fraud has been committed does not only consist of passports, but also, for example, driving licences, identity cards and residence permits. The share of the total taken up by passports, identity cards, residence permits, and refugee passports is shown in the tables and graphs below.

In Figure five is the distribution shown in absolute numbers and in Figure six in percentage numbers. It can be concluded from this that identity cards have become a more popular document to commit fraud over the years. In both Figure five and six it can be seen that the share taken up by identity cards is rising sharply. In the latter period the share taken by identity cards and passports is even equal, while in the first and second period the share taken by passports is clearly much larger than the share taken by identity cards.

Fraud committed	2004	2004	2005	2005	2006	2006
	%	N	%	N	%	N
Passport	71,4	2028	73,7	1737	76,6	1444
Identity card	10,9	310	11,3	266	11,1	209
Residence permit	13,5	383	15,0	354	12,3	231
Passport refugees	1,2	34	1,3	31	1,2	23
Fraud committed	2007	2008	2008	2009	2009	2010
	N	%	N	%	N	%
Passport	932	65,0	867	66,8	589	62,5
Identity card	200	15,9	212	13,6	120	17,6
Residence permit	156	7,4	99	6,6	59	6,3
Passport refugees	16	1,5	20	1,5	13	1,6

Fraud committed	2011	2011	2012	2012	2013	2013
	%	N	%	N	%	N
Passport	64,5	733	59,2	477	57,6	492
Identity card	15,5	176	20,2	163	19,4	166
Residence permit	8,3	94	6,3	51	7,5	64
Passport refugees	1,4	16	1,5	12	0,8	7

Fraud committed	2014	2014	2015	2015	2016	2016
	%	N	%	N	%	N
Passport	43,9	508	62,5	688	53,2	502
Identity card	27,1	314	17,6	193	34,2	323
Residence permit	4,7	54	6,3	70	9,9	94
Passport refugees	1,7	20	1,8	20	1,9	18

Fraud committed	2017	2017	2018	2018	2019	2019
	%	N	%	N	%	N
Passport	50,6	559	47,6	562	45,4	555
Identity card	34,9	386	38,5	455	36,7	449
Residence permit	8,9	98	7,2	85	7,4	91
Passport refugees	2,3	25	2,5	30	2,5	31

Fraud committed	2020	2020
	%	N
Passport	42,8	436
Identity card	40,8	416
Residence permit	7,7	78
Passport refugees	2,5	25

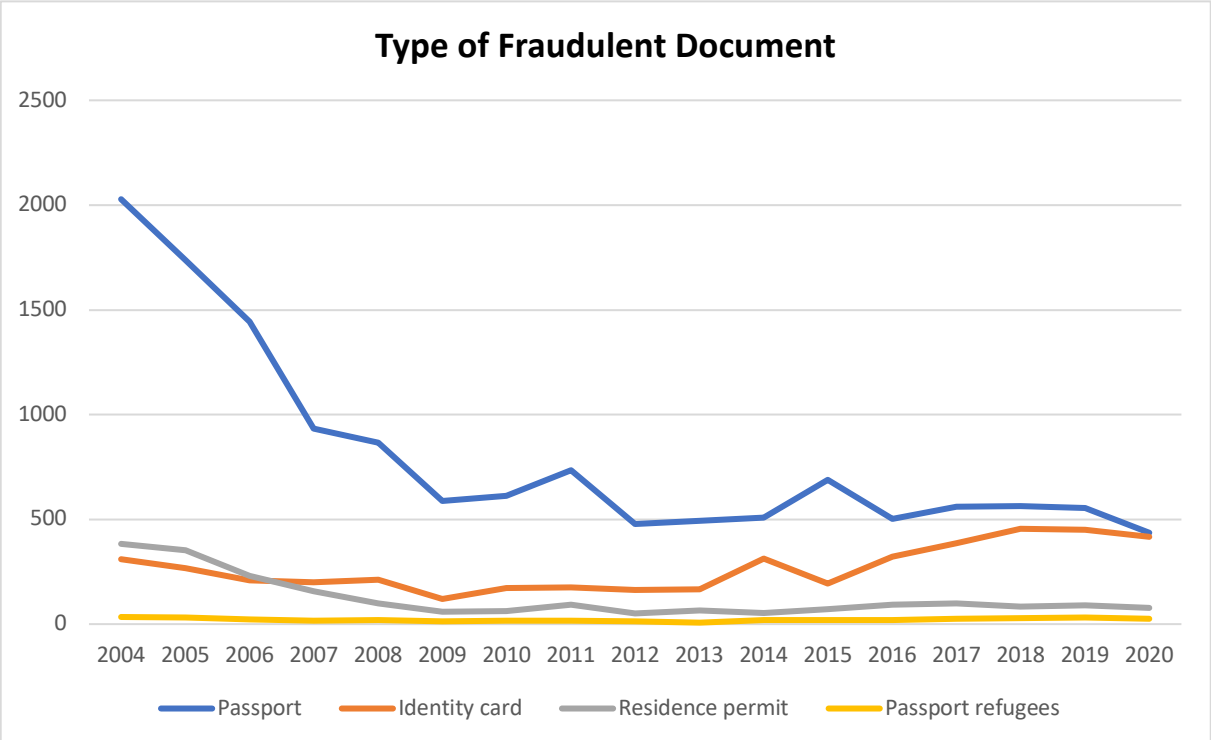

Figure 5, Type of fraudulent document

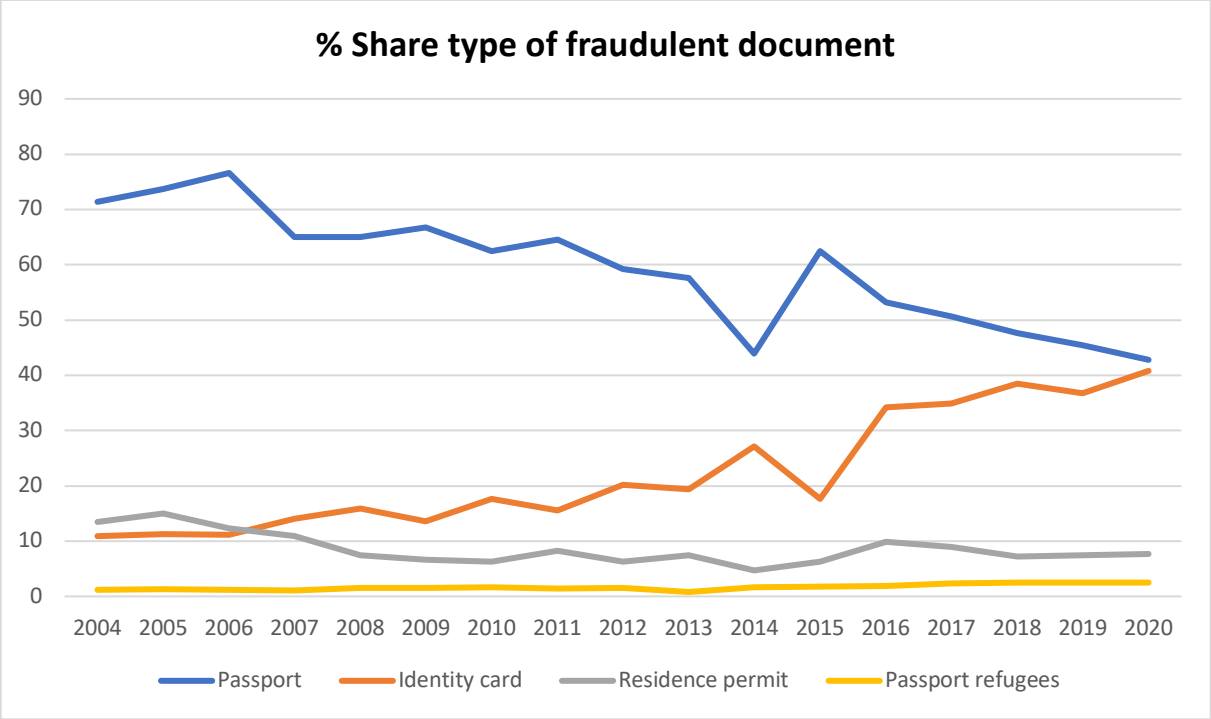

Figure 6, % Share type of fraudulent document

Type of document fraud

As described earlier, the ECID distinguishes between three different types of document fraud. These are counterfeit, fake and good/authentic documents. The tables below show the type of fraud as a percentage. In the first time period the average number of counterfeit documents is 62.9%, in the second time period this number has decreased to 50.9%. In the last time period, the average number of counterfeit documents has decreased further to 40.9%. This clear decline over the years must result in an increase elsewhere. This upward trend can be found in both the intercepted fake and the intercepted good/authentic documents but is predominant in the fake documents type. In the first period, the average number was 17.4%, while in the last period it increased to 33.7%, so it almost doubled.

Type of document fraud in %	2004	2005	2006	2007	2008	2009	2012
Counterfeit	61,3	62,0	65,4	52,5	54,2	51,6	56,7
Fake	17,4	18,1	16,7	26,4	22,6	22,7	27,2
Good/Authentic	21,2	19,9	18,0	21,1	23,2	25,7	16,1

Type of document fraud in %	2010	2011	2012	2013	2014	2015
Counterfeit	53,8	54,3	56,7	54,0	41,5	49,4
Fake	23,8	24,9	27,2	27,4	30,0	29,1
Good/Authentic	22,4	20,8	16,1	18,6	28,5	21,5

Type of document fraud in %	2016	2017	2018	2019	2020
Counterfeit	41,3	47,7	39,7	38,3	37,9
Fake	29,0	26,5	35,4	36,3	36,5
Good/Authentic	19,7	25,7	24,9	25,4	25,6

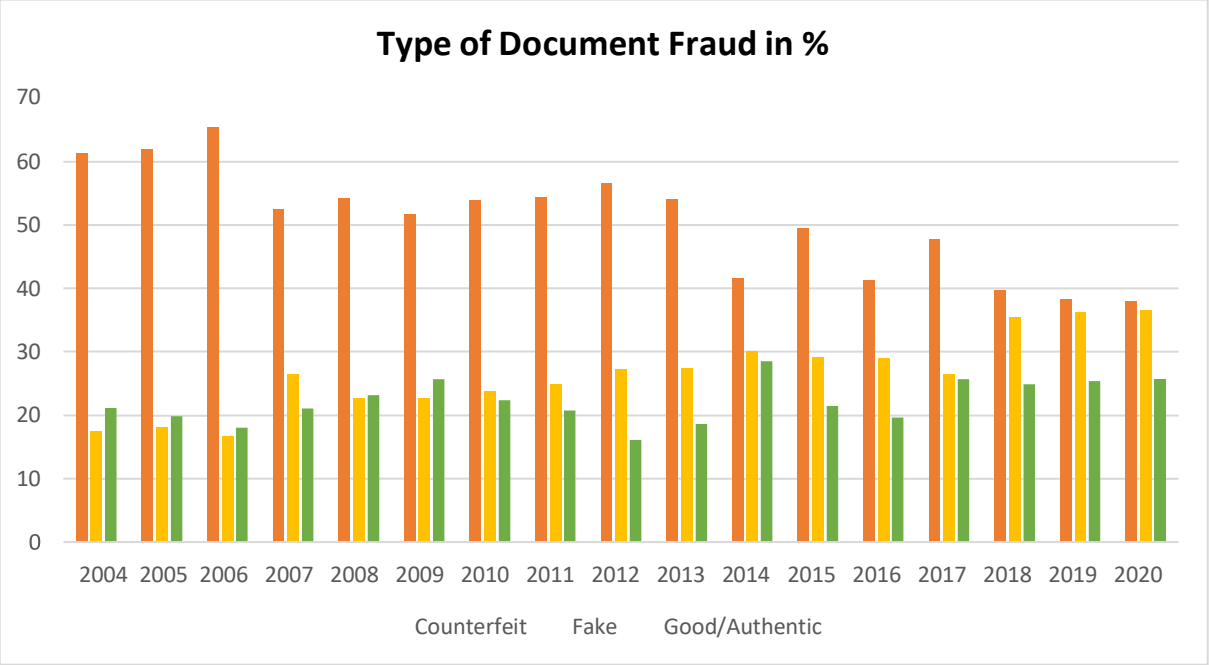

Figure 7, Type of Document fraud in percentages

In absolute numbers, a strong decrease in all categories is visible, however, this is the case because the total number of intercepted documents that have been used to commit fraud is also in a declining trend. In the table below these numbers are shown in a table and in Figure eight these numbers are shown in a graph, which leads to the conclusion that the share of the various types of document fraud is getting closer and closer to each other. Therefore, it can be concluded that there is a clear change visible in the type of fraud committed.

Type of document fraud in N	2004	2005	2006	2007	2008	2009
Counterfeit	1740	1462	1233	753	723	459
Fake	494	427	315	378	301	201
Good/Authentic	602	467	340	303	309	228

Type of document fraud in N	2010	2011	2012	2013	2014	2015
Counterfeit	527	617	457	461	481	543
Fake	233	283	219	234	347	320
Good/Authentic	219	236	130	159	330	237

Type of document fraud in N	2016	2017	2018	2019	2020
Counterfeit	390	526	469	468	386
Fake	274	292	418	443	372
Good/Authentic	186	284	294	310	261

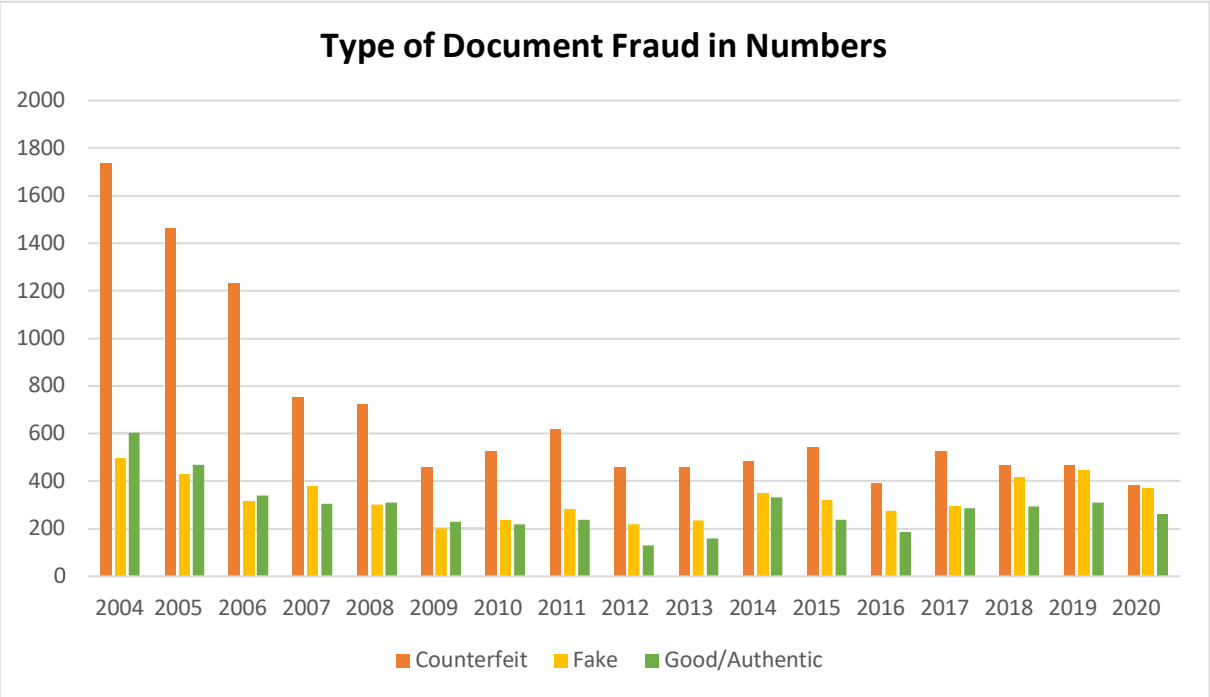

Figure 8, Type of Document fraud in Numbers

Modus Operandi no resemblance

The RFID chip in e-passports contains biometric data of the owner, to prevent identity fraud, especially look-alike fraud. The modus operandi associated with this form of fraud is no resemblance/imposter and the statistics are shown in the table below. In absolute numbers, this modus operandi decreases enormously in time period two compared to the first time period, because the total number of documents with which fraud has been committed also decreases. Therefore, the percentage number is also showed in the table. In Figure nine this trend is visible in a graph and it can be seen that there is no clear decrease over the years. At the beginning of the first period, there is a downward trend noticeable, which turns into an upward trend when period two starts, halfway through the second time period the trend changes again into a downward trend and this wave continues until the end of the third time period.

Year	2004 - %	2004 - N	2005- %	2005 - N	2006 - %	2006 - N
Modus operandi No resemblance (Imposter)	14,9	423	13,4	315	13,1	247

Year	2007 - %	2007 - N	2008 - %	2008 - N	2009 - %	2009 - N
Modus operandi No resemblance (Imposter)	14,9%	214	15,4%	205	18,3	161

Year	2010 - %	2010 - N	2011 - %	2011 - N	2012 - %	2012 - N	2013 - %	2013 - N
Modus operandi No resemblance (Imposter)	17,3	170	13,6	154	11,5	92	12,2	104

Year	2014 - %	2014 - N	2015 - %	2015 - N	2016 - %	2016 - N	2017 - %	2017 - N	2018 - %	2018 - N
Modus operandi No resemblance (Imposter)	13,0	150	15,4	169	13,4	127	18,4	203	17,1	201

Year	2019 - %	2019 - N	2020 - %	2020 - N
Modus operandi No resemblance (Imposter)	18,5	218	18,6	189

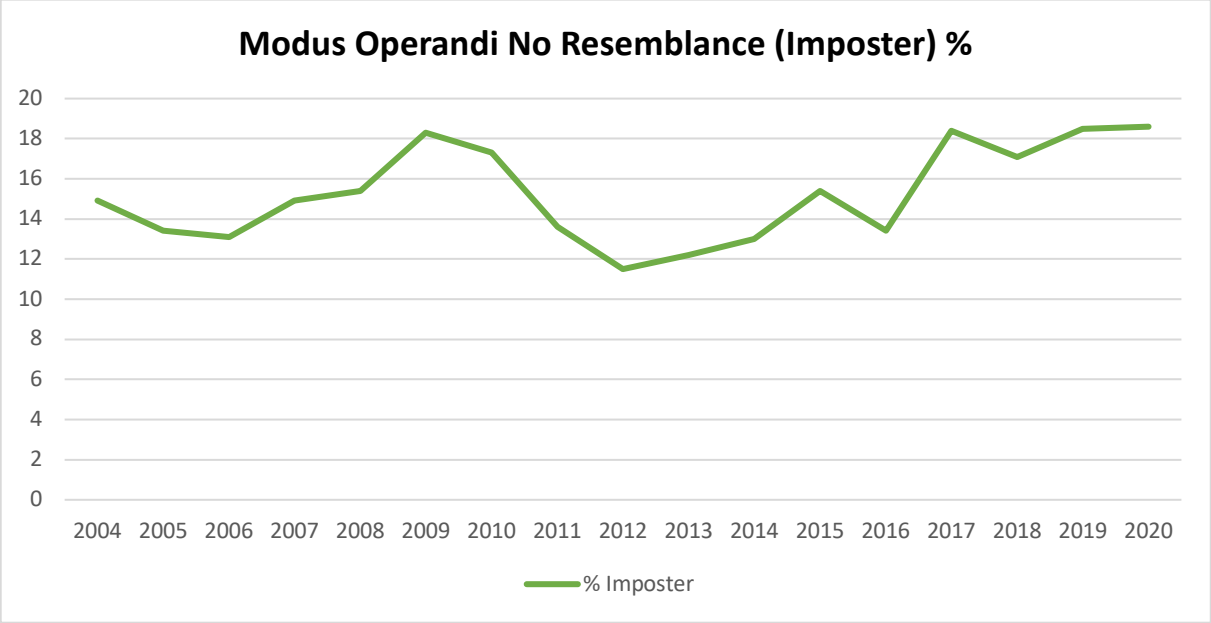

Figure 9, Modus Operandi Look-alike fraud

Dutch Documents

The figures in the ECID reports show the statistics for document fraud committed on Dutch territory. However, the tables and graphs contain the total number of document fraud committed, which means that no distinction is made between countries. This results in the fact that there is no clear cut-off detectable when the chip is implemented as it happened on a different date for each country.

Because it is clear when the RFID chip was implemented in the Netherlands, the available data on fraud committed with Dutch documents will receive some extra attention in this part of the study, since the ECID has devoted a separate chapter to fraud with Dutch documents.

In Figure ten, which belongs to the data from tables on page 42-48 a wave pattern is detectable when looking at the total number of Dutch documents with which fraud has been committed over the years. In Figure eleven the numbers are shown without the total amount so that it is clearer what the statistics are per type of document. The wave pattern is also clearly visible here. What is remarkable is the fact that the number of intercepted fraudulent passports and

identity cards, in contrast to the figures with the total numbers, has not grown closer together. The number taken up by passports in 2019-2020 is still clearly larger than the share of identity cards.

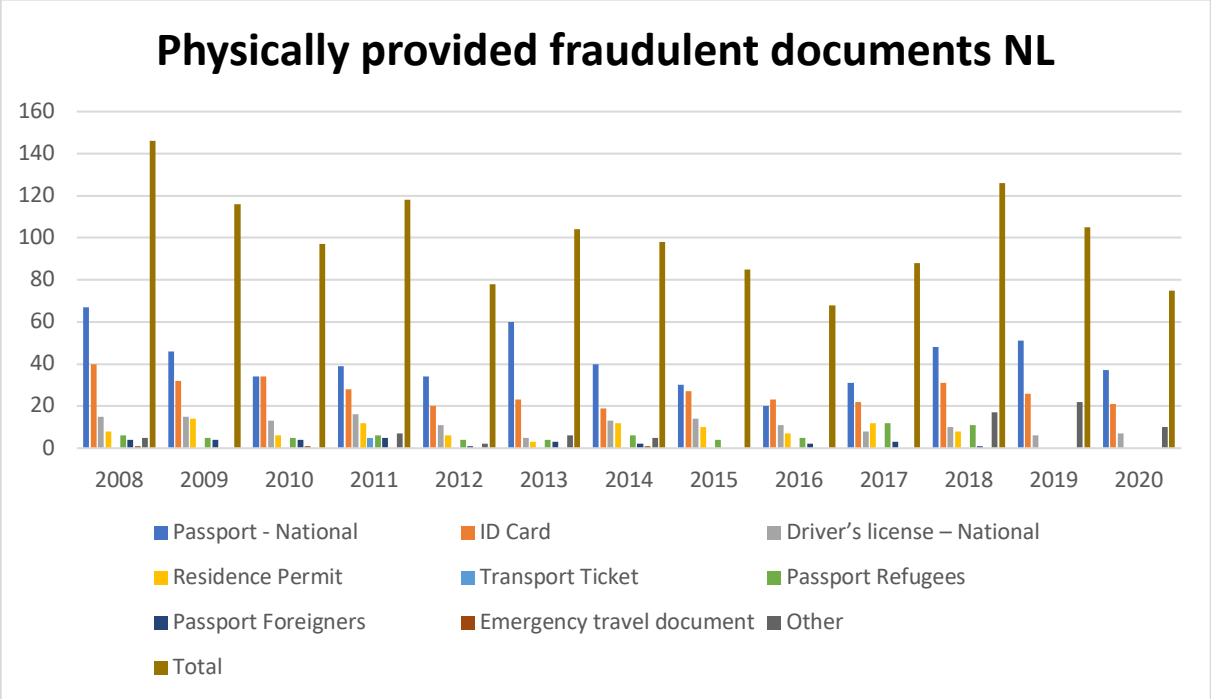

Figure 10, physically provided fraudulent documents NL

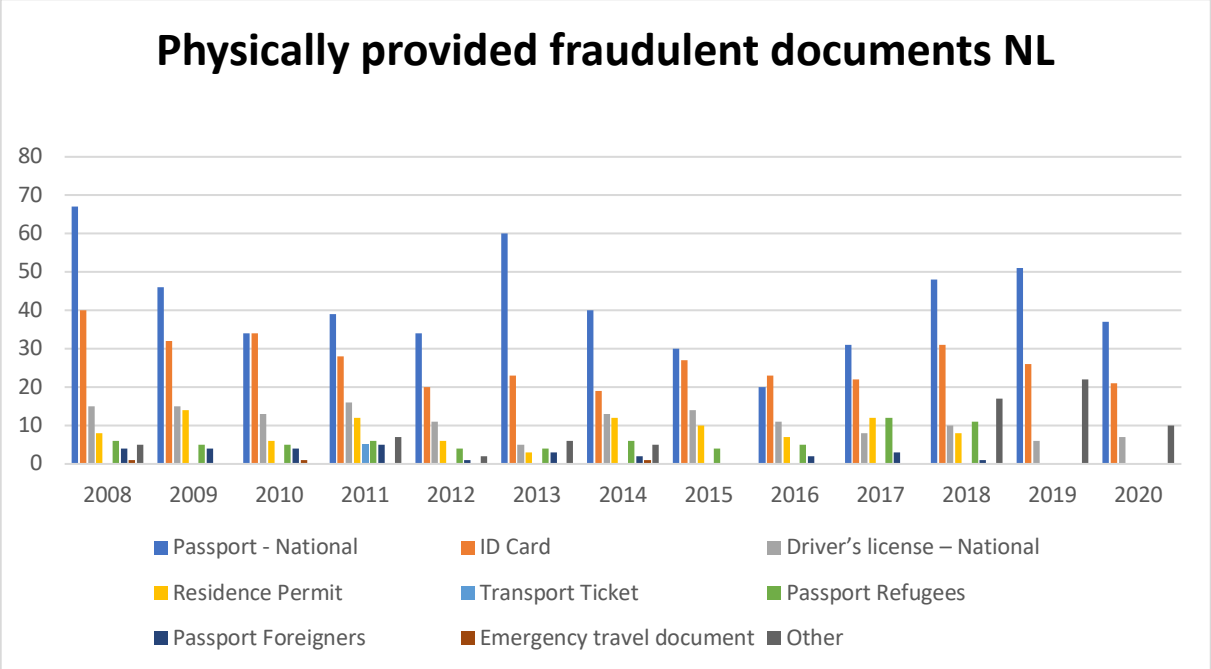

Figure 11, physically provided fraudulent documents NL without total

Physically provided fraudulent documents NL	2008	2008	2009	2009	2010	2010
Type of Document	N	%	N	%	N	%
Passport - National	**67**	**45,9**	**46**	39,7	**34**	35,1
ID Card	**40**	**27,4**	**32**	27,6	**34**	35,1
Driver's license – National	15	10,3	15	12,9	13	13,4
Residence Permit	8	5,5	14	12,1	6	6,2
Transport Ticket	0	0	0	0	0	0
Passport Refugees	6	4,1	5	4,3	5	5,2
Passport Foreigners	4	2,7	4	3,4	4	4,1
Emergency travel document	1	0,7	0	0	1	1,0
Other	5	3,4	0	0	0	0
Total	146	100	116	100	97	100

Physically provided fraudulent documents NL	2011	2011	2012	2012	2013	2013
Type of Document	N	%	N	%	N	%
Passport - National	**39**	33,1	**34**	43,6	**60**	57,7
ID Card	**28**	23,7	**20**	25,6	**23**	22,1
Driver's license – National	16	13,6	11	14,1	5	4,8
Residence Permit	12	10,2	6	7,7	3	2,9
Transport Ticket	5	4,2	0	0	0	0
Passport Refugees	6	5,1	4	5,1	4	3,8
Passport Foreigners	5	4,2	1	1,3	3	2,9
Emergency travel document	0	0	0	0	0	0
Other	7	5,9	2	2,6	6	5,8
Total	118	100	78	100	104	100

Physically provided fraudulent documents NL	2014	2014	2015	2015	2016	2016
Type of Document	N	%	N	%	N	%
Passport - National	**40**	40,8	**30**	35,3	**20**	29,4
ID Card	**19**	19,4	**27**	31,7	**23**	33,8
Driver's license – National	13	13,3	14	16,5	11	16,2
Residence Permit	12	12,2	10	11,8	7	10,3
Transport Ticket	0	0	0	0	0	0
Passport Refugees	6	6,1	4	4,7	5	7,4
Passport Foreigners	2	2,0	0	0	2	2,9
Emergency travel document	1	1,1	0	0	0	0
Other	5	5,1	0	0	0	0
Total	98	100	85	100	68	100

Physically provided fraudulent documents NL	2017	2017	2018	2018	2019	2019
Type of Document	N	%	N	%	N	%
Passport - National	**31**	35,2	**48**	38,1	**51**	48,6
ID Card	**22**	25,0	**31**	24,6	**26**	24,8
Driver's license – National	8	9,1	10	7,9	6	5,7
Residence Permit	12	13,6	8	6,3	0	0
Transport Ticket	0	0	0	0	0	0
Passport Refugees	12	13,6	11	8,7	0	0
Passport Foreigners	3	3,5	1	0,9	0	0
Emergency travel document	0	0	0	0	0	0
Other	0	0	17	13,5	22	20,9
Total	88	100	126	100	105	100

Modus operandi Dutch documents

The tables and graphs below show for each year what the distribution has been among the different modus operandi. Specific focus is on the modus operandi no resemblance/imposter as this includes the numbers related to look-alike fraud. The other modus operandi are also visible in the tables, but in the graphs only the course for the modus operandi look-alike fraud is visible.

Figure twelve shows that the modus operandi look-alike fraud is decreasing for both passports and identity cards. This can be linked to the total number of document fraud committed in these years, which is also in a decreasing trend in these years, as can be seen in Figure eleven. Figure thirteen shows the numbers as a percentage, and here again a clear wave pattern is visible, which makes it possible to conclude that no apparent decrease is detectable in the modus operandi no resemblance/imposter which includes look-alike fraud.

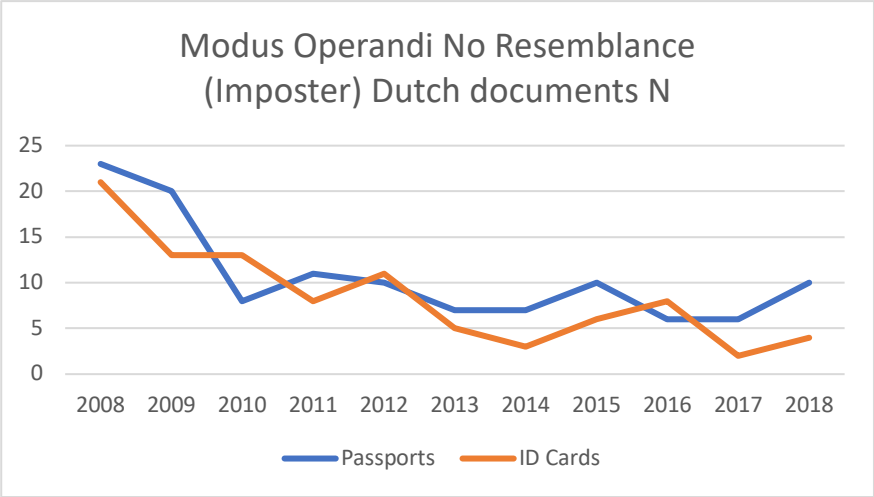

Figure 12, modus operandi look-alike fraud Dutch documents in numbers

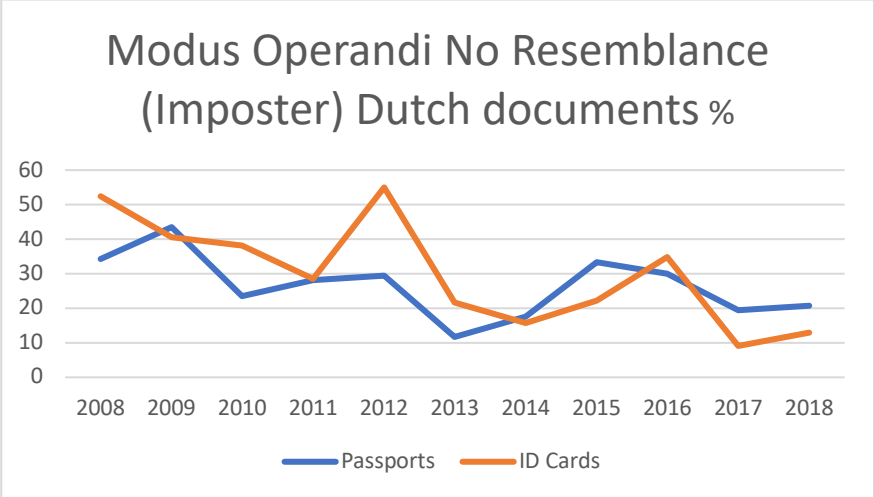

Figure 13, modus operandi look-alike fraud Dutch documents in percentages

	MO NL passports	2008	2008	2009	2009	2010	2010
Type of Document	Modus operandi	N	%	N	%	N	%
Counterfeit	Personal details page false	19	28,4	8	17,4	5	14,7
	Page removed	9	13,4	0	0	0	0
	Page replaced	1	1,5	1	2,2	0	0
	Blank Stolen	0	0	1	2,2	0	0
	Photo replaced	0	0	1	2,2	1	2,9
	Fake stamp	2	3,0	0	0	1	2,9
	Personal details p. forged	1	1,5	3	6,5	2	5,9
	Variable data falsified	0	0	0	0	0	0
	Personal details p. replaced	1	1,5	1	2,2	0	0
	Damaged / Destroyed	0	0	0	0	0	0
	Visa forged	0	0	0	0	1	2,9
	Other counterfeits	5	7,5	11	23,9	15	44,1
Total		37	55,2	25	54,3	25	73,5
Good	No resemblance (imposter)	23	**34,3**	20	**43,5**	8	**23,5**
	Stolen/missing	6	9,0	0	0	0	0
	Fraudulently obtained	1	1,5	1	2,2	1	2,9
Total		30	44,8	21	45,7	9	26,5
Fake	Totally false	0	0	0	0	0	0
Total		0	0	0	0	0	0
	Total	**67**	**100**	**46**	**100**	**34**	**100**

	MO NL passports	2011	2011	2012	2012	2013	2013
Type of Document	Modus operandi	N	%	N	%	N	%
Counterfeit	Personal details page false	10	25,6	13	38,2	23	38,3
	Page removed	0	0	0	0	0	0
	Page replaced	0	0	0	0	3	5,0
	Blank Stolen	0	0	0	0	0	0
	Photo replaced	1	2,6	0	0	9	15,0
	Fake stamp	2	5,1	0	0		
	Personal details p. forged	3	7,7	1	2,9	2	3,3
	Variable data falsified	0	0	0	0	0	0
	Personal details p. replaced	0	0	0	0	0	0
	Damaged / Destroyed	0	0	0	0	0	0
	Visa forged	0	0	1	2,9	0	0
	Other counterfeits	11	28,2	7	20,6	13	21,7
Total		27	69,2	22	64,7	50	83,3
Good	No resemblance (imposter)	11	**28,2**	10	**29,4**	7	**11,7**
	Stolen/missing	0	0	0	0	0	0
	Fraudulently obtained	0	0	1	2,9	1	1,6
Total		11	28,2	11	32,4	8	13,3
Fake	Totally false	1	2,6	1	2,9	2	3,3
Total		1	2,6	1	2,9	2	3,3
	Total	**39**	**100**	**34**	**94**	**60**	**100**

	MO NL passports	2014	2014	2015	2015	2016	2016
Type of Document	Modus operandi	N	%	N	%	N	%
Counterfeit	Personal details page false	4	10,0	2	6,7	0	0
	Page removed	0	0	0	0	1	5,0
	Page replaced	0	0	0	0	0	0
	Blank Stolen	0	0	0	0	0	0
	Photo replaced	3	7,5%	1	3,3	0	0
	Fake stamp	0	0	0	0	2	10,0
	Personal details p. forged	3	7,5	2	6,7	1	5,0
	Variable data falsified	0	0	2	6,7	0	0
	Personal details p. replaced	0	0	0	0	1	5,0
	Damaged / Destroyed	0	0	0	0	3	15,0
	Visa forged	0	0	0	0	0	0
	Other counterfeits	22	55,0	12	40,0	5	25,0
Total		32	80,0	19	63,4	13	65,0
Good	No resemblance (imposter)	7	**17,5**	10	**33,3**	6	**30,0**
	Stolen/missing	0	0	1	3,3	1	5,0
	Fraudulently obtained	1	2,5	0	0	0	0
Total		8	20,0	11	36,6	7	35,0
Fake	Totally false	0	0	0	0	0	0
Total		0	0	0	0	0	0
	Total	**40**	**100**	**30**	**100**	**20**	**100**

	MO NL passports	2017	2017	2018	2018	2019	2020
Type of Document	Modus operandi	N	%	N	%	N	N
Counterfeit	Personal details page false	1	3,2	2	4,2		
	Page removed	1	3,2	3	6,3		
	Page replaced	0	0	0	0		
	Blank Stolen	0	0	0	0		
	Photo replaced	0	0	8	16,7		
	Fake stamp	1	3,2	0	0		
	Personal details p. forged	0	0	4	8,3		
	Variable data falsified	2	6,5	1	2,1		
	Personal details p. replaced	0	0	0	0		
	Damaged / Destroyed	7	22,6	7	14,6		
	Visa forged	0	0	0	0		
	Other counterfeits	12	38,7	11	22,9		
Total		24	77,4	36	75,1		
Good	No resemblance (imposter)	6	**19,4**	10	20,8		
	Stolen/missing	0	0	0	0		
	Fraudulently obtained	1	3,2	0	0		
Total		7	22,6	10	20,8		
Fake	Totally false	0	0	2	4,1		
Total		0	0	2	4,1		
	Total	**31**	**100**	**48**	**100**	**51**	**37**

	MO NL ID Cards	2008	2008	2009	2009	2010	2010
Type of Document	Modus operandi	N	%	N	%	N	%
Counterfeit	Personal details page false	0	0	1	3,1	0	0
	Page removed	0	0	0	0	0	0
	Page replaced	0	0	0	0	0	0
	Blank Stolen	1	2,5	2	6,3	0	0
	Photo replaced	0	0	0	0	2	5,9
	Fake stamp	0	0	0	0	0	0
	Personal details p. forged	0	0	0	0	1	2,9
	Variable data falsified	0	0	0	0	0	0
	Personal details p. replaced	0	0	0	0	0	0
	Damaged / Destroyed	0	0	0	0	0	0
	Visa forged	0	0	0	0	0	0
	Other counterfeits	0	0	0	0	1	2,9
Total		1	2,5	3	9,4	4	11,8
Good	No resemblance (imposter)	21	**52,5**	13	**40,6**	13	**38,2**
	Stolen/missing	0	0	0	0	0	0
	Fraudulently obtained	1	2,5	0	0	1	2,9
Total		22	55,0	13	40,6	14	41,2
Fake	Totally false	17	42,5	16	50,0	16	47,1
Total		17	42,5	16	50,0	16	47,1
	Total	**40**	**100**	**32**	**100**	**34**	**100**

	MO NL ID Cards	2011	2011	2012	2012	2013	2013
Type of Document	Modus operandi	N	%	N	%	N	%
Counterfeit	Personal details page false	3	10,7	0	0	0	0
	Page removed	0	0	0	0	0	0
	Page replaced	0	0	0	0	0	0
	Blank Stolen	0	0	0	0	0	0
	Photo replaced	0	0	0	0	0	0
	Fake stamp	0	0	0	0	0	0
	Personal details p. forged	0	0	0	0	0	0
	Variable data falsified	0	0	0	0	0	0
	Personal details p. replaced	0	0	0	0	0	0
	Damaged / Destroyed	0	0	0	0	0	0
	Visa forged	0	0	0	0	0	0
	Other counterfeits	1	3,6	0	0	2	8,7
Total		4	14,3	0	0	2	8,7
Good	No resemblance (imposter)	8	**28,6**	11	**55,0**	5	**21,7**
	Stolen/missing	0	0	0	0	0	0
	Fraudulently obtained	0	0	0	0	0	0
Total		8	28,6	11	55,0	5	21,7
Fake	Totally false	16	57,1	9	45,0	16	69,6
Total		16	57,1	9	45,0	16	69,6
	Total	**28**	**100**	**20**	**100**	**23**	**100**

	MO NL ID Cards	2014	2014	2015	2015	2016	2016
Type of Document	Modus operandi	N	%	N	%	N	%
Counterfeit	Personal details page false	0	0	0	0	0	0
	Page removed	0	0	0	0	0	0
	Page replaced	0	0	0	0	0	0
	Blank Stolen	0	0	0	0	0	0
	Photo replaced	0	0	1	3,7	2	8,7
	Fake stamp	0	0	0	0	0	0
	Personal details p. forged	0	0	0	0	0	0
	Variable data falsified	1	5,3	0	0	1	4,3
	Personal details p. replaced	0	0	0	0	0	0
	Damaged / Destroyed	0	0	1	3,7	0	0
	Visa forged	0	0	0	0	0	0
	Other counterfeits	0	0	0	0	2	8,7
Total		1	5,3	2	7,4	5	21,6
Good	No resemblance (imposter)	3	**15,8**	6	**22,2**	8	**34,8**
	Stolen/missing	0	0	1	3,7	0	0
	Fraudulently obtained	2	10,5	0	0	0	0
Total		5	26,3	7	25,9	8	34,8
Fake	Totally false	13	68,4	18	66,7	10	43,5
Total		13	68,4	18	66,7	10	43,5
	Total	**19**	**100**	**27**	**100**	**23**	**100**

	MO NL ID cards	2017	2017	2018	2018	2019	2019	2020	2020
Type of Document	Modus operandi	N	%	N	%	N	%	N	%
Counterfeit	Personal details page false	0	0	1	3,2				
	Page removed	0	0	0	0				
	Page replaced	0	0	0	0				
	Blank Stolen	0	0	0	0				
	Photo replaced	2	9,1	1	3,2				
	Fake stamp	0	0	0	0				
	Personal details p. forged	0	0	0	0				
	Variable data falsified	3	13,6	3	9,7				
	Personal details p. replaced	0	0	0	0				
	Damaged / Destroyed	0	0	2	6,5				
	Visa forged	0	0	0	0				
	Other counterfeits	1	4,5	2	6,5				
Total		6	27,2	9	29,1				
Good	No resemblance (imposter)	2	**9,1**	4	**12,9**				
	Stolen/missing	0	0	0	0				
	Fraudulently obtained	0	0	0	0				
Total		2	9,1	4	12,9				
Fake	Totally false	14	63,7	18	58,0				
Total		14	63,7	18	58,0				
	Total	**22**	**100**	**31**	**100**				

Type of Travel Document	Date	Number in Circulation
Dutch Passport	01-01-2016	9183788
Dutch Passport	01-01-2017	9333375
Dutch Passport	01-01-2018	9362493
Dutch Passport	01-01-2019	9466408
Dutch Passport	01-01-2020	9812486
Dutch Passport	01-01-2021	9916804
Dutch Identity Card	01-01-2016	7503904
Dutch Identity Card	01-01-2017	7206848
Dutch Identity Card	01-01-2018	7432670
Dutch Identity Card	01-01-2019	7535870
Dutch Identity Card	01-01-2020	7780212
Dutch Identity Card	01-01-2021	7847292

Type of Travel Document	Year	Total number issued
Dutch Passport	2011	1698345
Dutch Passport	2012	2158947
Dutch Passport	2013	1852767
Dutch Passport	2014	1921787
Dutch Passport	2015	1791918
Dutch Passport	2016	1892977
Dutch Passport	2017	2169372
Dutch Passport	2018	1886446
Dutch Passport	2019	769456
Dutch Passport	2020	392661
Dutch Identity Card	2011	2127880
Dutch Identity Card	2012	1497960
Dutch Identity Card	2013	1215549
Dutch Identity Card	2014	1348173
Dutch Identity Card	2015	1610522
Dutch Identity Card	2016	1805716
Dutch Identity Card	2017	1725586
Dutch Identity Card	2018	1333303
Dutch Identity Card	2019	694039
Dutch Identity Card	2020	543695

Summary Interview

On Tuesday 9 December from 9am to 10am, the interview with two ECID employees took place via MS Teams. These employees were Mrs. Lonneke Bontje and Mr. Alexander Castanon.

First, an introduction round took place in which explanations were given about the research and permission was requested to make a sound recording. During the proposal round, Mr. Castanon introduced himself first. He has been working at ECID since 2009 and previously studied Criminology at Leiden University. He started as an analyst at the ECID and has now been working for several years in the Consultancy & Development department, where he is also the head of the bureau. He then linked his position to the research question of this report and said that there are some people within the Royal Military Police who have studied biometrics, the RFID chip and its control. Finally, he added that he was the right person to ask for clarification about the RFID chip and its control.

Ms Bontje introduced herself as head of the analysis bureau, and senior analyst at ECID. She started working for the Marechaussee in 2012 and has since then fulfilled various analysis functions, including: the types of crime at the airports and immigration flows. She has been working for ECID since 2019. She also said that this organization is mainly concerned with the trends and developments in identity fraud committed with documents. Identity fraud also takes place on, for example, marketplaces, where people use data from others to place orders, for example. This does not belong to the scope of the ECID because the ECID looks at issues at an operational, tactical, and strategic level.

After the proposal round, I shared my screen and showed the results of the literature review. This showed that the implementation of the chip in passports involved a lot of privacy and security issues. The main reason for the implementation was the fight against look-alike fraud, but whether the benefits outweigh all the security risks was still unclear. Mrs. Bontje and Mr. Castanon answered this question as follows:

The terms that came up, which could be a possible privacy leak or could be seen as weaknesses, are known and extra security measures have been introduced. The implemented security measures such as basic access authentication, active authentication and passive authentication

have been developed against the potential threats and are good enough to ensure that the vulnerabilities can be prevented. If a country (issuing authority) assembles the chip properly and carries out the check in the right way, this is sufficient to guarantee the security of the chip. On the leak of biometric data, he added that a photo of the passport holder can also be obtained by viewing a physical passport, so it makes no difference compared to an e-passport with a chip containing the same photo. He said that fingerprints, which he believes are more sensitive than the photo, are also extra protected. This extra protection has even led to the fact that the fingerprints could not even be used in practice until now. Finally, he elaborated on the term cryptographic weakness. According to him, certain protections are also being further developed to ensure that the cryptographic protections that are now on the chip cannot be cracked, an example of this is the switch from BAC to PACE. What Mr. Castanon then talked about is that he has seen some presentations about quantum computers lately. These could pose a danger to the chips in passports. Quantum computers are a new kind of computers that are currently being worked on, so they are not a legitimate threat for issues like identity fraud yet, but it is expected that they will come on the market and that they can pose a major threat to e-passports. This danger arises because the chip can then be cracked fairly easily.

The second part of the interview focused on the results. The data from the ECID's reports on document fraud has been shown to Ms Bontje and Mr Castanon with the statement that the numbers are quite low and there is no apparent decrease in the number of cases involving fraud involving passports with an RFID chip. Rather, there has been a 'wave movement' over the years. So, gradual decreases and increases, but no obvious decrease. The chip is mainly implemented to prevent look-alike fraud, but even when looking at the modus operandi 'imposter', there is no clear decrease. Ms Bontje and Mr Castanon were asked whether the implementation of the chip had a positive effect on identity fraud. To this Ms Bontje replied the following.

The figures are indeed low, but that has to do with the fact that certain documents are used more or less to commit fraud, which depends on various influences. Numerous variables influence the figures, such as the frequency of checks, availability, and the desired final destination of a migrant. For example, because of the Schengen Act (free movement of goods and persons in the EU), only 1 flight per day from a certain country may be checked. Mr Castanon added that the e-passport has indeed been implemented for the main purpose of combating imposters. Another, not entirely unimportant reason that he still wanted to address was automation. Due

to the implementation of the chip, checking travellers at the airport is currently also possible via a machine. This is much faster and many times more reliable than physical checks.

Overall analysis

Number in graph	Analysed case	Time period 1	Time period 2	Time period 3
1	Average number cases/suspected persons FSD Schiphol Desk	2298	748	836
2	Average number intercepted fraudulent documents	2361	1062	1131
3	Average share of intercepted fraudulent documents taken up by passports	73,9	53,5	46,6
4	Average share of intercepted fraudulent documents taken up by identity cards	11,1	18,1	37,7
5	Average share of intercepted fraudulent documents taken up by type of document fraud counterfeit	62,9	56,6	40,9
6	Average share of intercepted fraudulent documents taken up by type of document fraud fake	17,4	29	33,7
7	Average share of intercepted fraudulent documents taken up by type of document fraud good	19,7	23,4	25,4
8	Average share of intercepted fraudulent documents taken up by modus operandi no resemblance	10,4	14,5	18,15

Looking at all the years for which data has been collected, since 2006 there has been no clear decrease or increase in the cases in which identity fraud has been committed with a travel document. Before the implementation date of the chip, there is a very clear decrease visible, but this finding is not related to the implementation of the chip.

What is striking is that there has been a wave movement in the number of cases of identity fraud, from 2001 a sharp decrease is visible, but around 2009 the line starts to rise again, before falling again in 2011 and this goes further in this trend. The same trend can be found for the modus operandi look-alike fraud, in both the percentage and absolute analysis.

Another striking finding is that the number of fraudulent identity cards in relation to the total number of documents intercepted has increased considerably over the years. The increase is so great that in 2020 the number of cases involving identity fraud with a passport was almost equal to the number of cases involving an identity card.

If we look specifically at the Dutch documents with which identity fraud has been committed, the same trend is visible. Here, too, a wave pattern can be observed in both the number of fraudulent documents that have been intercepted and the modus operandi look-alike fraud.

Case three to eight are shown visually in the graph below. The average number of the cases/suspected persons reported to the FSD Schiphol Desk at Schiphol, and the average number of intercepted fraudulent documents have been omitted because they were already in a strong downward trend before the implementation of the chip and thus cannot be used to draw conclusions. Figure fourteen, which belongs to the table above, also only contains figures about all cases of identity fraud committed on Dutch territory. A distinction or separate analysis of only Dutch documents was superfluous and unreliable since only Dutch documents are distinguished from 2008 and the chip was already implemented in 2006.

As showed in Figure fourteen, there is a decreasing trend noticeable for the average share of intercepted fraudulent documents taken up by passports (number three) and an increasing trend for the average share of intercepted fraudulent documents taken up by identity cards (number four). There is also a decreasing trend in the average share of intercepted fraudulent documents taken up by type of document fraud counterfeit (number five), this decreasing trend results in an increasing trend in the average share of intercepted fraudulent documents taken up by type

of document fraud fake (number six). Number seven, which includes the average share of intercepted fraudulent documents taken up by type of document fraud good, remains almost the same. This type of document fraud also includes the modus operandi no resemblance, which can be seen in Figure fourteen under number eight. Just like the type of document fraud under which this modus operandi falls, the number of cases in which look-alike fraud has taken place remains on the same level (only a very slight increase can be detected).

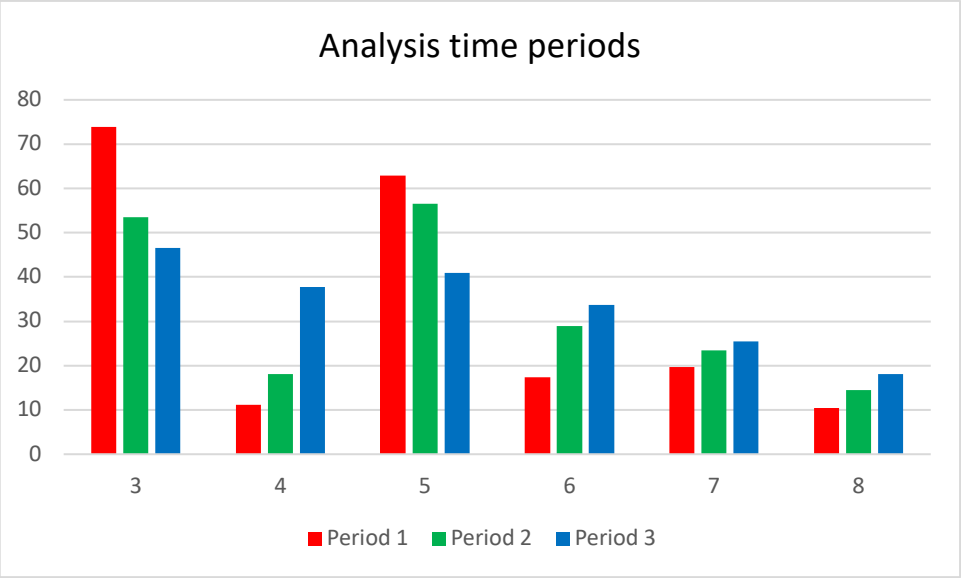

Figure 14, Analysis showed in time periods

Conclusion

The main goal of the implementation of an RFID chip in passports was to combat look-alike fraud by adding biometric data of the document holder to the chip. The implementation of e-passports was and still is accompanied by security and privacy issues, which has led to a strong discussion of the pros and cons in recent years.

It was expected that the size of the committed identity fraud would decrease sharply in the years after the implementation of the chip. However, this is not clearly reflected in the results, so the hypotheses are rejected. The magnitude of identity fraud committed on Dutch territory was already in a downward trend before the chip's implementation date, which continued at the start of the introduction, but cannot be traced back to the implementation of the RFID chip. The additional privacy and security issues compared to the unclear decrease in the magnitude of identity fraud could argue that the introduction of e-passports has led to more adverse than beneficial consequences. However, the efficiency associated with the introduction of e-passports is of enormous importance. The rapid passage of passengers at airports is a huge advantage. Nevertheless, the fact remains that the level of identity fraud has not clearly decreased with the implementation of the chip. In addition, the modus operandi no resemblance, which includes look-alike fraud, has not decreased significantly in percentage terms compared to the other forms of identity fraud, so neither can be concluded that a shift has occurred in the modus operandi.

Discussion

Validity

The conclusion of this report is based on identity fraud committed on Dutch territory. Because every country has different control requirements for e-passports, the results cannot be generalized.

The method used to answer the research question, namely the analysis of the ECID's annual reports containing the statistics on identity fraud on Dutch territory, is a reliable method. However, the reports only contain numbers from the most involved organization in the field of identity fraud on Dutch territory, the Royal Netherlands Marechaussee. This can be seen as a limitation because the Marechaussee in the Netherlands does not have a monopoly on handling document fraud. The police regions, the Immigration and Naturalization Service (IND) and the Customs also do this. Currently, there is not enough information available for the ECID about the identity fraud intercepted by other services to be able to make reliable statements about this. Developments are underway that should improve the information position of the ECID in this area so that this data can also be included in the reports.

Another limitation is that the intercepted fraudulent documents provided by other institutions (banks or municipalities) are not only tested at the helpdesks that are linked to the ECID. Some organizations use their own document specialists. For example, the Amsterdam-Amstel land region has a Team Identity/Document Fraud (TIF) since March 2008. Also, from the private sector not all institutions and companies make use of the counterfeit desks. For example, they can also make use of commercial institutions that provide the same type of services for a fee to check documents.

Results

The results of the study do not fully match the hypotheses. According to the hypothesis, the number of people committing look-alike fraud with a passport should decrease in the years after the chip's implementation. This cannot be traced from the results.

In the interview Ms Bontje and Mr Castanon, gave a possible clarification for this untraceable decrease, namely that not every flight from the Schengen area may be checked at Schiphol and that not all cases involving identity fraud are reported to the various reporting centres of the

Royal Netherlands Marechaussee. The first clarification is being questioned because the Schengen Agreement was already signed on 14 June 1985 by the heads of government of Belgium, the Netherlands, Luxembourg, Germany, and France and officially entered into force on 26 May 1995. This means that this law has been in effect for 11 years before the chip was implemented and therefore has no influence on the results of this study, as data from 2001 onwards is being analysed.

The second argument of Mrs. Bontje and Mr. Castanon can indeed influence the research results, because not every case of fraud ends up with the Marechaussee and therefore not all cases are included in the annual reports that have been analysed for this study.

Recommendations

The research has shown that implementing an RFID chip with biometric data in passports mainly works for efficiently checking travellers at the airport. By means of the chip, it is possible to use e-Gates, which means that faster and better passport controls can take place.

The implementation of the chip to combat identity fraud, in particular look-alike fraud, cannot be proved based on the results of this study. There is no clear decrease in the extent and nature of identity fraud.

Moreover, the implementation of the chip entails many privacy and security issues. These are well covered in the security measures, but it has also emerged that the use of the fingerprint as a biometric data on the chip does not actually occur yet, but it does cause a stir. That is why the advice is to further investigate whether the implementation of a fingerprint on the chip is necessary.

Bibliography

A. Juels. (2006, February 2). *RFID Security and Privacy: A Research Survey.* Retrieved October 2021, from Research Gate: file:///Users/marleenhoorn/Documents/Scriptie/juels2006.pdf

Atkins & Yu. (2011, September). *Privacy and security protection of RFID data in e-passport*. Retrieved October 2021, from Research Gate: https://www.researchgate.net/publication/254009407_Privacy_and_security_protection_of_RFID_data_in_e-passport

Atzori et al. (2010, October 28). *The Internet of Things: A survey.* Retrieved January 2022, from Elsevier: https://www.sciencedirect.com/science/article/pii/S1389128610001568?casa_token=R_ArySwD9XUAAAAA:ZDnavQ1fWUMuV84CzsPyHRwVxmacoKsM2skrLQTxda8iWYuPtCxdgRdrzbxT1KsJ8TK-WZxNTGY

Babich, A. (2012). *Biometric Authentication. Types of biometric identifiers.* Retrieved November 2021, from Haage-Helia University: https://www.theseus.fi/bitstream/handle/10024/44684/Babich_Aleksandra.pdf

Baum, K. (2006, April). *First Estimates from the National Crime Victimization Survey Identity Theft.* Retrieved November 2021, from Prison Policy: https://static.prisonpolicy.org/scans/bjs/it04.pdf

Bobkowska, K. (2019, October 23). *Incorporating iris, fingerprint and face biometric for fraud prevention in e-passports using fuzzy vault.* Retrieved October 2021, from The Institution Of Engineering and Technology : https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-ipr.2019.0072

Bocchetti, S. (2006, July). *Security and Privacy in RFID Protocols.* Retrieved November 2021, from Penn State University : http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.598.8406&rep=rep1&type=pdf

Bogari et al. (2012). *An Analysis of Security Weaknesses in the Evolution of RFID Enabled Passport.* Retrieved November 2021, from International Journal of Internet Technology and Secured Transactions: https://sci-hub.se/https://www.inderscienceonline.com/doi/pdf/10.1504/IJITST.2012.054060

Bogari et al. (2012, June). *An Analysis of Security Weaknesses in the Evolution of RFID Enabled Passport.* Retrieved November 2021, from Research Gate: https://www.researchgate.net/publication/259647269_An_Analysis_of_Security_Weaknesses_in_the_Evolution_of_RFID_Enabled_Passport

Broek, E. v. (2010). *Beyond Biometrics.* Retrieved November 2021, from Elsevier: https://reader.elsevier.com/reader/sd/pii/S1877050910002851?token=14EB5A11D636A3583CE1A7303FFD458DA8513107337F795329E6D8F8A774171CED0F5AAE9108F32DFB189073A7A66E86&originRegion=eu-west-1&originCreation=20211110113525

Brookman et al. (2010). Handbook on Crime. In F. B. al., *Handbook on Crime.* Willan Publishing.

Brummelkamp, G. (2020, February). *Monitor Identiteit*. Retrieved November 2021, from Rijksoverheid: file:///Users/marleenhoorn/Downloads/Monitor+Identiteit+2019.pdf

C.J.F. Williams. (1989). What is Identity? In Williams, *What is Identity?* Retrieved from Clarendon Press.

Consumer Financial Protection Bureau. (n.d.). *Learn More.* Retrieved November 2021, from Comnsumer Finance: https://www.consumerfinance.gov/learnmore/

Coosemans, D. (2020, February 14). *Veelbesproken e-gates op luchthaven.* Retrieved January 2022, from Nieuwsblad: https://www.nieuwsblad.be/cnt/dmf20200213_04847594

Deng, F. (1995). War of Visions: Conflict of Identities in the Sudan. Washington DC: Brookings.

Derksen. (2009, November 15). *Ons lichaam ter beveiliging van onze materiële eigendommen?* Retrieved November 2021, from Dutchpelican: http://www.dutchpelican.com/uploads/6/3/4/0/63400561/20091115_biometrie.pdf

Domdouzes et al. (2007, October). *Radio-Frequency Identification (RFID) applications: A brief introduction.* Retrieved November 2021, from Elsevier: https://www.sciencedirect.com/science/article/pii/S1474034606000498?casa_token=5hAYiswLalUAAAAA:c3hblZTZjnUF56ATpprnGbm3efH13LJEgz8soKQFPbftX54SyGo3kCqiq6z_k6gnyhc4k6_ZQnU

Ehrsam et al. (1978). *A cryptographic key management scheme for implementing the Data Encryption Standard.* Retrieved November 2021, from IEE Xplore : https://ieeexplore.ieee.org/abstract/document/5388038

Enahoro, B. (2019). Global Cyber Security Labor Shortage and International Business Risk.

FCRA. (2018, September). *Fair Credit Reporting Act.* Retrieved November 2021, from https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf

Geenens, S. (2014). *IDENTITEITSDIEFSTAL: NOODZAAK AAN EEN WETGEVENDE TUSSENKOMST?* Retrieved December 2021, from https://libstore.ugent.be/fulltxt/RUG01/002/163/144/RUG01-002163144_2014_0001_AC.pdf

Grijpink . (2004, January). *Identity fraud as a challenge to the constitutional state.* Retrieved November 2021, from Elsevier: https://www.sciencedirect.com/science/article/pii/S0267364904000068?casa_token=zgCC9Ja_7OAAAAAA:0mPtgGSDQeIGJLhK93UCjUac3zLG8PkR8nWNPgJ_papBTl7F33sSLm9N3VSGjnImPw451LOQ9ZM

Grijpink, J. (2005). *Biometrics and identity fraud protection: Two barriers to realizing the benefits of biometrics – A chain perspective on biometrics, and identity fraud – Part II.* Retrieved October 2021, from Elsevier: https://www.sciencedirect.com/science/article/abs/pii/S026736490500097X?casa_token=lGlSgozkJIQAAAAA:kPjJ6LqdMLMQ7fro-Ascsjfx-Bc2_pZ29_247zGGGxwQvYN0XfMUYmoqwTYhT4sBx6oQ93oFaQ

Hoepman et al. (2008, February). *Crossing Borders: Security and Privacy Issues of the European e-Passport.* Retrieved October 2021, from ResearchGate: https://www.researchgate.net/publication/1908323_Crossing_Borders_Security_and_Privacy_Issues_of_the_European_e-Passport

Hogg & Abrahams. (1988). Social Identifications: A Social Psychology of Intergroup Relations and Group Processes. London: Routledge .

Hyona, O. &. (2016, January). *Position tracking and identity tracking are separate systems: Evidence from eye movements.* Retrieved November 2021, from Elsevier: https://www.sciencedirect.com/science/article/pii/S0010027715300949

ICAO. (n.d.). *A-System Requirements*. Retrieved November 2021, from International Civil Aviation Organization: https://www.icao.int/Security/FAL/PKD/BVRT/Pages/System-Requirements.aspx

Jacobs, B. (2005). *Biomety in passports.* Retrieved October 2021

Jain et al. . (2008). handbook on Biometrics. New York: Springer Science & Business Media.

Juels et al. (2005, January). *Security and Privacy Issues in e-Passports*. Retrieved October 2021, from ResearchGate: https://www.researchgate.net/publication/221272981_Security_and_Privacy_Issues_in_E-passports/link/00b4953bbe2f619c72000000/download

Koninklijke Marechaussee. (2015, September). *Expertisecentrum Identiteitsfraude en Documenten en ID-desks*. Retrieved November 2021, from file:///Users/marleenhoorn/Downloads/Web_Folder+ECID_NL_2015.pdf

Kosmerlj, M. (2005). *Passport of the Future: Biometrics against Identity Theft?* Retrieved October 2021, from Norwegian University of Science and Technology: https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/143765/Kosmerlj_-_Passport_of_the_future-biometrics_against_identit.pdf?sequence=1

Kundra et al. (2014). *The study of recent technologies used in E-passport system.* Retrieved November 2021, from IEEE Global Humanitarian Technology Conference: https://sci-hub.se/https://ieeexplore.ieee.org/abstract/document/6967573

Lee, V. (2008). *Biometrics and Identity Fraud.* Retrieved October 2021, from Elsevier: https://www.sciencedirect.com/science/article/pii/S0969476508700596?casa_token=AFxwB_8z1NIAAAAA:mLgDkERHcFYrXZ8uz1ZYN-V-7kV60noTq__p4kRAijmLPcVA_3cuEYylwjmnPGSzgs_3wOQ98Bs

Lekkas, D. (2007, June). *E-Passports as a Means Towards the First World-Wide Public Key Infrastructure.* Retrieved December 2021, from Research Gate : https://www.researchgate.net/publication/221406395_E-Passports_as_a_Means_Towards_the_First_World-Wide_Public_Key_Infrastructure

leyden, J. (2006). *RFID hack attack: E-passport cloning risks exposed.* Retrieved November 2021, from The Register: https://www.theregister.com/2006/08/04/e-passport_hack_attack/

LoPucki, L. (2001, May 3). *Human Identification Theory and the Identity Theft Problem.* Retrieved November 2021, from SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=263213

Müller, H. &. (2008, July). *Characteristics of Personality and Identity in Population Surveys: Approaches for Operationalising and Localizing Variables to Explain Life Satisfaction.* Retrieved November 2021, from Research Gate: https://www.researchgate.net/publication/250962011_Characteristics_of_Personalit

y_and_Identity_in_Population_Surveys_Approaches_for_Operationalising_and_Localizing_Variables_to_Explain_Life_Satisfaction

Ministerie van Binnenlandse Zaken en Koninklijksrelaties. (2013, December 12). *Identiteit in Cijfers* . Retrieved November 2021, from Kennis Openbaar Bestuur : https://kennisopenbaarbestuur.nl/media/53882/identiteit-in-cijfers.pdf

National Office for Identity. (2020). *Over RvIG.* Retrieved November 2021, from Ministerie van Binnenlandse Zaken en Koninklijksrelaties: https://www.rvig.nl/over-rvig

Nithyanand, R. (2009, January). *A Survey on the Evolution of Cryptographic Protocols in ePassports.* Retrieved November 2021, from Research Gate: https://www.researchgate.net/profile/Rishab-Nithyanand/publication/220334365_A_Survey_on_the_Evolution_of_Cryptographic_Protocols_in_ePassports/links/5565aa1a08aec4b0f485b2e4/A-Survey-on-the-Evolution-of-Cryptographic-Protocols-in-ePassports.pdf

Panteia. (2015). *Monitor identiteit in cijfers.* Retrieved November 2021, from Panteia: https://panteia.nl/onderzoeken/monitor-identiteit-in-cijfers/

Pattinson. (2021, August 12). *How the world's most secure ID documents protect trust and privacy.* Retrieved October 2021, from BiometricUpdate: https://www.biometricupdate.com/202108/how-the-worlds-most-secure-id-documents-protect-trust-and-privacy

Pattinson, N. (2004). *Securing and Enhancing the Privacy of the e-Passport with contactless electronic chips.* Retrieved October 2021

R. Leenes. (2006). *Identity Theft, Identity Fraud and/or Identity-related Crime.* Retrieved December 2021, from DuD: https://sci-hub.se/https://link.springer.com/article/10.1007/s11623-006-0141-2

Ramya et al. (2018). *Biometric Authentication to ensure security in ePassports.* Retrieved January 2022, from IEE Xplore: https://ieeexplore.ieee.org/abstract/document/8668170

Rijksoverheid. (2020). *Centraal Bureau voor de Statistiek (CBS).* Retrieved November 2021, from Rijksoverheid: https://www.rijksoverheid.nl/contact/contactgids/centraal-bureau-voor-de-statistiek-cbs

Rijksoverheid. (n.d.). *Welke organisaties mogen een kopie van mijn identiteitsbewijs maken?* Retrieved December 2021, from Rijksoverheid:

https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/vraag-en-antwoord/ben-ik-verplicht-om-een-kopie-van-mijn-identiteitsbewijs-te-geven-aan-een-bedrijf

Royal Dutch Marechaussee. (2020, February). *Statistisch jaaroverzicht van identiteits- en documentfraude in 2019.* Retrieved November 2021, from Ministry of Defense: https://www.privacyfirst.nl/images/stories/WOB/ECID/Statistisch_overzicht_documentfraude_2019.pdf

Schouten, B. (2008, May 13). *Biometrics and their use in e-passports*. Retrieved October 2021, from Elsevier: https://sci-hub.se/https://www.sciencedirect.com/science/article/abs/pii/S0262885608001200?casa_token=Gwvg82VI16MAAAAA:JzbPXN2d0iWcf7XbPQll9j__ZG7UNCl-ouC3r5pkJxUMm78Shr7V6hgpM49QN4NpHDPBbFBiXVo

Schuchter & Levi. (2013). *The Fraud Triangle Revisited.* Retrieved November 2021, from Research Gate: https://www.researchgate.net/publication/271270579_The_Fraud_Triangle_Revisited

Singel, R. (2005, February 24). *No Encryption for E-Passports*. Retrieved October 2021, from Wired: https://www.wired.com/2005/02/no-encryption-for-e-passports/

Snijder, M. (2010, November). *Het Biometrisch Paspoort in Nederland Crash of Zachte Landing.* Retrieved January 2022, from Library Open: https://library.oapen.org/bitstream/handle/20.500.12657/33961/439976.pdf?sequence=1

Suhaimi et al. (2020). *Assessment of Malaysian E-Passport PKI based on ISO 27000 Series International Standards.* Retrieved November 2021, from Journal of Physics: https://iopscience.iop.org/article/10.1088/1742-6596/1551/1/012003/pdf

Thompson et al. (2006). *RFID security threat model.* Retrieved January 2022, from netgeek: https://netgeekdr.com/wp-content/papercite-data/pdf/9023.pdf

Weis, S. (2007). *RFID (Radio Frequency Identification): Principles and Applications.* Retrieved January 2022, from Stitcs: http://stitcs.com/EN/RFID/RFID%20Principles%20and%20Applications.pdf

Williams, B. (1956). *Personal Identity and Individuation*. Retrieved November 2021, from Jstor: https://www.jstor.org/stable/pdf/4544578.pdf

Xiao et al. (2009). *RFID Technology, Security Vulnerabilities, and Countermeasures.* Retrieved January 2022, from Research Gate: https://www.researchgate.net/profile/Qinghan-Xiao/publication/221787702_RFID_Technology_Security_Vulnerabilities_and_Countermeasures/links/0f31752e2823d63b6b000000/RFID-Technology-Security-Vulnerabilities-and-Countermeasures.pdf

Appendix

Interview Transcript

Marleen Hoorn (00:01)
Ik zal me er eerst zelf bij voorstellen en het hele verhaal achter mijn onderzoek toelichten en daarna kunnen jullie vertellen wat je in die functie is. Ik doe dus de Master Economics en Governance aan de Universiteit Leiden. En nu hoef ik dus alleen nog maar mijn scriptie te schrijven, die doe ik dus over identiteitsfraude. Ik zit bij de capstone technologie in the public sector. Dus het moest gerelateerd zijn aan technologie en dan gecombineerd met bijvoorbeeld beleid.

Dus ik ben uiteindelijk gegaan voor de paspoorten met de chip die in 2006 in Nederland zijn geïmplementeerd. En dan onderzoek ik dus wat de impact daarvan is op identiteitsfraude. En dan dus met look-alike fraude omdat er natuurlijk zo'n chip met biometrische gegevens in zit. Ik zal mijn scherm even delen.

Zien jullie mijn scherm?

Alexander Castanon (01:38)
Ja, ja.

Marleen Hoorn (01:40)
Jullie zien hier dus de titelpagina van mijn scriptie dus mijn scriptie met de hoofdvraag: What Was the Effect of the Implementation of an RFID-chip in Passports on the Rate of Detected Identity Fraud in The Netherlands. De scripotie schrijf ik dus in het Engels, maar het interview kan gewoon in het Nederlands. En dan heb ik hier dus al een introductie en een onderzoeksvraag en de al bestaande literatuur gereviewed. Voor de resultaten heb ik dus de Statistical Annual Reports gebruikt van het expertisecentrum waar jullie voor werken. Die heb ik allemaal gefilterd op bruikbare gegevens, wat een hele taak was. Maar uiteindelijk ben ik op deze tabellen als resultaten gekomen. Het ding waar ik dus wel tegenaan met gelopen is dat er maandrapport zijn vanaf 2008, omdat het expertisecentrum daarvoor nog niet bestond.Maar ik heb wel gelezen dat er daarvoor een andere naam had, en dat het nationaal bureau van de documenten daarvoor zelf de cijfers heeft bijgehouden. En in één van de rapporten stond dus ook deze grafiek, dat er dus al wel data is vanaf 2001 2002. Dus ik vroeg me af of er een manier is om daar nog aan te komen of dat er daar andere rapporten van zijn.

Alexander Castanon (03:47)
Dan kijk ik even naar Lonneke.

Lonneke Bontje (03:52)
Sorry, ik heb er geen weet van dat er rapporten zijn van voor 2008 omdat het ECID toen nog niet bestond. Daarnaast hebben wij een bewaartermijn dus deze gegevens kunnen wij ook niet meer verstrekken, mochten ze wel beschikbaar zijn.

Alexander Castanon (04:43)
Ja helaas kunnen we die data niet zomaar meer kunnen opvragen in verband met de bewaartermijn en dat soort dingen.

Marleen Hoorn (04:53)
Ja, nee begrijp ik, want hiervoor heette het inderdaad natuurlijk ook anders. En ik weet niet hoe dat zit met alle takken. Want de data van voor die tijd is dus afkomstig van een organisatie die nu niet meer bestaat. Is er nog iemand die ik daarvoor kan contacteren of kom ik dan weer bij het ECID uit?

Alexander Castanon (05:19)
Ja, danm kom je eigenlijk weer terug bij het expertisecentrum.

Marleen Hoorn (05:22)
Dus het heeft geen zin om apart daar mensen van te contacteren?

Alexander Castanon (05:27)
Nee, die data is ook al te oud om nog te delen. Die kunnen wij zelf ook niet zomaar weer opvragen.

Marleen Hoorn (05:38)
Nee, begrijp ik.

Nou, dit is dan dus de achtergrondinformatie. Dus dan zou ik graag willen weten wat jullie achtergornd is en wat jullie takenpakket en functieomschrijving bij het ECID is.

Alexander Castanon (05:50)
Ik werk vanaf 2009 bij het ECID en begon als analist, dit heb. Ik een paar jaar gedaaan en toen doorgegroeid. Inmiddels werk ik al heel wat jaartjes bij de afdeling advies en ontwikkeling en innovatie en ontwikkeling. Wij geven dus advies op allerlei gebieden zoals apparatuur en techniek, maar ook wet en regelgeving, opleidingen, trainingen, een stukje kennis, ontwikkeling. En de link naar jouw stuk is dat er binnen de KMar een aantal mensen zijn die zich hebben verdiept in onderwerpen als de chip en de controle daarvan.

Lonneke Bontje (07:35)
Dank je wel ja, ik ben werkzaam als Bureauhoofd van het bureau analyse, tevens senior analist bij het ECID. Net als Alexander heb ik criminologie in gestudeerd. Eerst in Amsterdam en daarna in Leiden. In 2012 begonnen bij de KMar en ik heb eigenlijk sinds die tijd verschillende analyse functies vervuld. Vaak voor de sectie lucht, dus alle criminaliteit voor op de luchthavens en vreemdelingen stromen. Daarna ben ik richting de ondermijnende criminaliteit gegaan en uiteindelijk nu al twee jaar werkzaam bij het ECID.

Wat wij voornamelijk doen is: wij houden ons bezig met trends en ontwikkelingen op het gebied van identiteitsfraude. Eigenlijk wel specifiek identiteitsfraude gepleegd met documenten. Je hebt natuurlijk ook identiteitsfraude, bijvoorbeeld op Marktplaats, waarbij iemand die gegevens die op internet staan gebruikt om zich als iemand anders voor te doen. Dat is iets minder onze tak van sport. Eigenlijk kijken wij naar vraagstukken op operationeel, tactisch en strategisch niveau.

Dus strategisch zit wat meer op het beleid, tactisch is het de creatie en operationeel voor de aansturing van onze eigen eenheden.

Marleen Hoorn (09:03)
Dus met de cijfers waar je niet bijvoorbeeld mee komen. Daar wordt ook beleid op gebaseerd?

Alexander Castanon (09:10)
Euh ja zeker. Ja, bijvoorbeeld die jaaroverzichten waarvan je er ook een aantal hebt gebruikt voor je scriptie. Die komen, onder anderen bij ons vandaan en worden bijvoorbeeld ook gebruikt voor de creatie van eventuele beleidsplannen op strategisch niveau.

Marleen Hoorn (09:25)
OK, interessant. Even kijken, zien jullie mijn scherm nog?

Alexander Castanon (09:37)
Ja.

Marleen Hoorn (09:48)
Ja, ik discussieer dus ook over de sterke en de zwakke punten van het paspoort, omdat het natuurlijk is ingevoerd tegen look-alike fraude. Echter kwamen hier best wel wat extra security en privacy dingetjes bij kijken. En volgens de literatuur die ik dus heb bestudeerd zijn dit een aantal van die bijkomende gevaren. Zoals dus natuurlijk skimming tracking, het klonen en het lekken van biometrische data, wat best wel veel is ten opzichte van de voordelen. In mijn optiek. Euhm, hoe zien jullie dat?

Alexander Castanon (10:41)
Ja, ik zie het staan inderdaad. Maar ik zie ook een aantal maatregelen staan die je hebt beschreven zoals BAC en active authenticationen die zijn juist gecreëerd om deze gevaren tegen te gaan. Dus om te voorkomen dat je langs iemand loopt die een apparaat heeft waarmee alle gegevens van jouw paspoort zomaar gelezen kunnen worden. Ik ben ervan overtuigd dat als je als land, dus als uitgevende instantie de controles op de juiste manier uitvoert dan de beveiliging dan heel sterk is. En ja het is vrij makkelijk om een chip van een paspoort uit te lezen. Er zijn ook gewoon apps waarmee dat kan, al zijn de gegevens die dan inzichtelijk gemaakt worden wel beperkt. Maar stel iemand heeft jouw foto en geboortedatum. Als je iemand op FaceBook toevoegt, heb je deze gegevens eigenlijk ook al in handen.

Dan hebben we natuurlijk nog de vingerafdrukken die in een paspoort zitten. Deze informatie ligt natuurlijk wel een stukje gevoeliger dan een foto of geboortedatum. Maar dit heeft er eigenlijk ook toe geleid dat deze gegevens in de parktijk eigenlijk nog helemaal niet gebruikt worden.

Marleen Hoorn (12:56)
OK, ja, duidelijk dus jij vindt dat de beveiligingsmaatregelen voldoende zijn om de potentiële gevaren op te vangen eigenlijk?

Alexander Castanon (13:10)
Ja dat vind ik zeker. Je ziet inderdaad dat hackers steeds meer nieuwe manieren proberen te vinden om de chip te kraken maar tegelijkertijd worden de beveiligingsmaatregelen ook continu doorontwikkeld en zijn deze up-to-date en van het hoogste niveau.

Wat wel een mogelijk gevaar kan vormen, daar heb ik zelf laatst een presentatie over gezien. Dat zijn quantum computers. Die zijn zo slim dat de chip dan eigenlijk wel te kraken en te veranderen valt. De chip kan dan op een relatief makkelijkere wijze gekraakt te worden, wat dus ook betekent dat het makkelijker wordt om een vals papsoort te maken. Maar die computers zijn nu nog in het beginstadium dus dat is nog lang niet van toepassing.

Marleen Hoorn (14:24)
Oh, daar heb ik nog niets over in mijn scriptie geschreven.

Alexander Castanon (14:33)
Oh, ja het staat nog in de kinderschoenen maar het is iets waar momenteel aan wordt gewerkt en het zou een potentieel gevaar kunnen opleveren. Maar ook tegen dit gevaar zijn er nu mensen beveiligingsmaatregelen aan het ontwikkelen die tegen die tijd zullen worden doorgevoerd.

Marleen Hoorn (15:22)
Wat is dan het tijdsbestek waar ik aan moet denken? Zijn deze computers er over 2 jaar of duurt dat nog decennia?

Alexander Castanon (15:33)
Ja dat is een lastige, ik denk dat je iets van 5 jaar in gedachten moet houden. Maar dit betekent dus ook dat er 5 jaar is om beveiligingsmaatregelen te ontwikkelen.

Marleen Hoorn (15:59)
Ja, ok, interessant.

Alexander Castanon (16:03)
Ik heb geen idee of daar iets over zou kunnen vinden.

Marleen Hoorn (16:10)
Oke bedankt, ja nu het gat in de onderzoekswereld. Er is dus veel research gedaan naar de voordelen en gevaren en nadelen etc. maar ik heb geen onderzoek gevonden met statische gegevens over fraude. Misschien komt dat omdat identiteitsfraude voor veel landen natuurlijk een gevoelig onderwerp is en landen dus niet transparant zijn in het delen van data. De fraude gepleegd op Nederlandse bodem is dus wel inzichtelijk. Dit komt alleen niet doordat het ECID deze data zelf heeft gedeeld. Privacy first heeft een WOB verzoek ingediend in 2012 en pas toen is de data openbaar gemaakt.

Alexander Castanon (17:19)
Ja klopt, de data was gewoon eerst niet openbaar. Ik zie hier trouwens iets over cloning staan en je bent ongetwijfeld artikelen tegengekomen waarin verhalen staan over mensen die een vals paspoort hebben gemaakt en hier dingen mee voor elkaar krijgen, en ja dat kan maar dat wil niet zeggen dat de beveiligingsmaatregelen niet goed zijn. Het kan ook aan de controlekant liggen. Als je bijvoorbeeld geen echte full of chip detection in een chip hebt. Er zijn landen die dat gewoon niet hebben. Dat is wereldwijd geen verplichting is. Ja dat, dan kan je die klonen. Dat is dan dus het risico van een land.

En als je een inspectiesystemen als een bepaalde beveiliging niet uitvoert. Ja, dan zou je er misbruik van kunnen maken. Maar als je de juiste beveiligingen implementeert en je

inspectiesystemen ook op de goede manier werken en al die beveiliging uitvoerbaar zijn, dan wordt dit echt heel lastig.

Marleen Hoorn (18:38)
Ja, dus. Het gaat er in ieder geval om of je ook controleert op de gevaren en dan zou je ze eruit kunnen pikken.

Alexander Castanon (18:47)
Jazeker, een makkelijk voorbeeld zijn bijvoorbeeld commerciële bedrijven die ook iets doen met de controle van documenten. Deze bedrijven kunnen bijvoorbeeld ook papsoortchips uitlezen. Zij krijgen dan inderdaad de data uit de chip van een ID of paspoort te zien maar dit zegt natuurlijk helemaal niets over de echtheid ervan. Alleen chip controlemechanismes met goede beveiligingsimplementaties bepalen nauwkeurig of een chip wel of niet echt is.

Marleen Hoorn (20:05)
Ja ja, dat zeker. Waar? Lonneke, heb jij hier nog iets aan toe te voegen?

Lonneke Bontje (20:15)
Nee eigenlijk niet, dit is meer Alexander zijn expertise en waar ik mij meer mee bezig houdt is het moment dat er fraude geconstateerd wordt.

Alexander Castanon (20:30)
OK

Marleen Hoorn (20:32)
Uhm, dank je wel. Dan wil ik nog even naar de resultaten gaan. Ik heb dus data vanaf 2008 terwijl het al in 2006 is geïmplementeerd. Dus daar moet ik nog even iets op gaan verzinnen. Maar in principe met deze data kan ik ook al conclusies trekken. Ja, hier in de tabel is het misschien wat onduidelijk te zien, maar ik ben bezig met het maken van deze grafieken. Dus ik heb dat al hier gedaan.

Ik zal het even kort toelichten. Zoal te zien is er is dus eigenlijk sprake van een soort golf beweging. Omdat het vanaf 2008 zijn de gevallen eigenlijk omlaag gegaan. Maar vanaf 2013 is er weer een piek en dan gaat het weer omlaag. En in 2018 is er weer een piek. Dan gaat het weer omlaag. En als ik de grafiek erbij pak waarin nog wel data te vinden is vanaf 2001, moet ik er wel bij zeggen dat dit in een grafiek is waarin de documenten is van alle nationaliteiten zijn verwerkt .

Maar als ik kijk naar de rapporten waar ik wel data heb van de Nederlandse en de documenten van alle andere nationaliteiten, is er best wel veel gelijkenis. Dus hier is ook al te zien dat er vanaf 2000 een piek is en er dan weer een daling. En vanaf 2011 stijgt het weer. Dus eigenlijk concludeer ik dan dat er niet echt een duidelijke afname is in de documenten waarmee fraude is gepleegd die worden onderschept. En als ik dan specifiek kijk naar de documenten waar dus look-alike fraude mee is gepleegd, dus wat gerelateerd kan worden aan de chip, hier heb ik dan alleen eventjes de paspoorten gedaan en heb het in het groen gezet. Dan, is er eigenlijk ook sprake van een niet echt duidelijke afname? Maar er zijn best wel veel pieken. En dan weer heel lage getallen. Dus ik concludeer dan dat er eigenlijk niet heel veel bereikt is op basis van lookalike fraude. En ook als ik kijk naar de getallen vind ik die best wel laag.

Dus in 2008 zijn er bijvoorbeeld 23 Nederlandse paspoorten onderschept waarmee dan look-alike Fraude is gepleegd in 2009 20, 2010 8, dus dan vraag ik me af of de reden dat het is geïmplementeerd dus de vermindering van imposters wel een echte goede grond is als de getallen zo'n laag zijn. Dus zijn eigenlijk twee vragen. Er is dus een golfbeweging te zien in de getallen van documenten waarmee fraude is gepleegd en de nummers waarmee look-alike fraude is gepleegd zijn best wel laag.

Dus of het wel echt een goede reden is geweest om de chip met biometrische gegevens te implementeren?

Lonneke Bontje (24:43)
Ik denk dat het laatste wat je zegt, dus dat het is misschien niet de goede reden geweest om die chip te implementeren, dat je die je echt moet nog moet loskoppelen van de cijfers die je hier ziet. De cijfers zijn inderdaad laag, en dat heeft ook te maken met het feit dat bepaalde documenten meer of minder gebruikt worden met verouderen. Dat is afhankelijk van van diverse invloeden, bijvoorbeeld de toename van vreemdelingen en vluchtelingen papsoorten. Ik weet niet of hier ook een chip in zit, Alexander?

Alexander Castanon (25:26)
Geen idee eigenlijk.

Lonneke Bontje (26:08)
Wat ik probeer te zeggen is dat je ook in je achterhoofd moet houden dat er een verschuiving is de laatste jaren in het gebruik van soorten documenten bij fraude.

Uhm, zou je eigenlijk, als je echt iets wil zeggen over die chip, dus niet specifiek naar de Nederlandse documenten moeten kijken, maar naar alle Europese documenten met een chip? 3 tot zou een veel betere doelgroep zijn met meer gegevens om daadwerkelijk een conclusie te trekken. Zoals dat je net schetst. Zeg maar die grillige bewegingen, ook met die kleine aantallen. Ook dat is lastig, want het is van zoveel invloeden afhankelijk. En als we maar beginnen over beschikbaarheid en over gewenste eindbestemming van een migrant.

En zo zijn er talloze variabelen die van invloed kunnen zijn op de keuze van het document. En daarnaast Nederlandse documenten worden niet alleen in Nederland natuurlijk, maar ook in het buitenland gebruikt.

Marleen Hoorn (27:23)
Ja ja, dat is zeker waar.

Lonneke Bontje (27:25)
Ja dus bij wijze van spreken. Wij hebben er misschien 1 onderschept in Nederland maar misschien wel 40 in Duitsland. Ja, en dat, dat is dan ook weer gelijk heel sterk van invloed op een eventuele conclusie trekt. Dus ik zou op basis van wat je nu hebt zou ik voorzichtig zijn en hebt bij wijze van spreken eerder aanbevelen naar breder onderzoek of getallen uit heel Europa laten onderzoeken.

Marleen Hoorn (27:56)
Ja.

Alexander Castanon (27:59)
Ja, dat was eigenlijk ook zo, zegt ik. Ik had twee punten dat we dit was de eerste. En je moet je voorstellen als ik als imposter op iemands anders papsoort wil reizen dan zou ik dan persoonlijk doen met een paspoort die niet afkomstig is uit het land waarin je fraude wil gaan plegen want daar kennen ze het document natuurlijk veel minder goed. Dat zou een reden kunnen zijn dat ze juist in het buitenland hogere cijfers hebben omtrent fraude met Nederlandse documenten dan in Nederland zelf.

Lonneke Bontje (28:40)
De toetsing ook met bijvoorbeeld taal. Jij hebt een Nederlands paspoort en jij spreekt geen Nederlands. Dat kan natuurlijk gewoon een enorme indicator zijn van het feit dat jij het niet bent en ja, in Duitsland zullen ze jou niet snel toetsen op je Nederlandse taal.

Marleen Hoorn (28:58)
Ja, nou is dit een goed punt, dan schrijf ik even op.

Lonneke Bontje (29:05)
Het zijn geen harde feiten maar het vermoeden bestaat wel dat fraude met Nederlandse documenten vooral buiten Nederland plaatsvindt.

Marleen Hoorn (29:22)
Ja dat is zeker een goed punt, ik zou ook eerder fraude plegen met een Nederlands document in het buitenland dan bijvoorbeeld in Schiphol.

Lonneke Bontje (30:26)
Er zit in alle criminaliteitscijfers wel een soort dark number. En dat is bijvoorbeeld ook als je kijkt binnen toen. Modus operandi die we de laatste jaren hebben gezien is bijvoorbeeld dat deze documenten voornamelijk gebruikt worden binnen het Schengen gebied. Binnen Schengen zijn er ook regels over hoeveel controles je mag doen. Dus stel dat je in maar 1 vlucht per dag mag controleren, dan moet de imposter daar maar net op zitten.

Bovendien is via het vliegtuig reizen voor fraudeurs vele malen riskanter dan bijvoorbeeld reizen over land in een auto en kleine binnendoor weggetjes nemen. De kans dat ze daar aan een controle worden onderworpen is natuurlijk veel kleiner.

Marleen Hoorn (31:33)
En waarom is daar een limiet aan opgesteld dan? Het controleren van de vluchten uit Schengen gebieden.

Lonneke Bontje (31:36)
Dat komt door het Schengenverdrag. Dit betekent vrij verkeer binnen de EU. Dus je mag bijvoorbeeld maar 1 vlucht uit Griekenland controleren terwijl Athene een bron is van migratiefraude.

Marleen Hoorn (32:23)
Ja oh, dat wist ik niet.

Lonneke Bontje (32:26)
Het is een voorbeeld dat alles allemaal afhankelijk is van de vlucht, frequentie en dat soort dingen. Daarbij bijvoorbeeld bankfraude, dit wordt niet altijd gemeld als het gebeurd is. En als het al wordt gemeld is het de vraag of het in de cijfers terecht komt. Of het dus wordt gemeld ja of nee.

Je kan je allerlei scenario's voorstellen. Bijvoorbeeld het moment waarop fraude aan de balie van een bank wordt geconstateerd. Eer er gebeld is, is de persoon in kwestie misschien al weggerend met het frauduleuze document Het klinkt allemaal eenvoudig, maar er zijn echt wel wat stappen die gezet moeten worden voordat het document dat onecht is, wordt onderschept en geteld.

Marleen Hoorn (34:08)
Ja, en denken jullie dat die golfbeweging waar ik het over had dat dat dan ook te wijten is aan bijvoorbeeld dat er de ene keer meer is gecontroleerd dan de andere keer? Of zou dat een andere reden kunnen hebben?

Lonneke Bontje (34:22)
Ik gaf wel aan dat het natuurlijk dat er heel veel variabelen van invloed zijn en ook de controle intensiteit kan daar een onderdeel van uitmaken.

Marleen Hoorn (34:32)
Dus dat er bijvoorbeeld in 2009 veel minder gecontroleerd is en bijvoorbeeld nu dan waar ik dan tegenaan loop. Van 2000, 19 en 20 waren de cijfers extreem laag, maar dat komt waarschijnlijk dan omdat er natuurlijk veel minder gereisd is door Corona.

Lonneke Bontje (34:52)
En ja, ja, dat kan, maar ik wil echt benadrukken dat je moet oppassen met zulke conclusies want in corona is het aantal onderschepte migratiedocumenten juist want er zijn minder migratie gerelateerde incidenten onbekend. Maar in verhouding zijn het er echt veel meer. Als je het afzet tegen het vliegverkeer. Het vliegverkeer is misschien wel met 90 procent afgenomen, maar het aantal ontkenningen bijvoorbeeld maar met 20 procent. Dus in verhouding heb je dan veel meer bijzonderheden gehad dan normaal.

Marleen Hoorn (35:28)
Ja ja. OK, schrijf ik ook even op.

Lonneke Bontje (35:34)
Dus het is wel heel belangrijk om dit allemaal in context te blijven zien en dat is eigenlijk een punt. Je kan eigenlijk niet denken aan hoeveel variabelen van invloed zou kunnen zijn, want het zijn er waarschijnlijk ontzettend veel.

Marleen Hoorn (35:50)
Ja ja. Dat is natuurlijk wel moeilijk te achterhalen allemaal.

Lonneke Bontje (35:57)
Nee, maar t is dat zou iets kunnen zijn voor waarom je bij wijze van spreken niet hele duidelijke conclusies kunt trekken.

Marleen Hoorn (36:04)
Nu ja, ja, ik kan natuurlijk sowieso denk niet echt een duidelijke conclusie maken omdat er simpelweg data ontbreekt van de jaren ervoor. En het is natuurlijk in 2006 ingevoerd. Dus uhm ja, als ik euh, als het daarvoor extreem laag was of extreem hoog, dan had ik misschien nog iets kunnen zeggen. Maar dan kunnen er inderdaad nog meer dingen van invloed zijn geweest. Alleen nu heb ik die data natuurlijk niet. Zo moet even gaan kijken hoe ik maar daaronder echt gaaf praten.

Maar ja, dan heb ik in ieder geval wel wat meer uitleg op de dingen die ik ook heb gevonden. Als ik vond het zelfs sommige dingen wel moeilijk te interpreteren, maar dat snap ik. Daar kunnen dus wel meerdere dingen op van invloed zijn.

Alexander Castanon (37:16)
Ik heb trouwens nog een punt. Ik zie dat je continu praat over biometrie op de chip tegen imposters en dat dat de reden is voor de chip maar er is ook een hele belangrijke andere reden zoals aqutomatisering heb je hier iets over geschreven>

Marleen Hoorn (37:32)
Euh ja, misschien heel klein, maar ik zou het wel fijn vinden als je er misschien verder op ingaat, want ik heb voornamelijk gefocust op biometrie zodat landen het Amerikaanse hun Visa Wever programma konden blijven. En als ze dat dan niet zou doen, dan zou het dus voor moeilijker worden om naar Amerika te reizen. En dat dat echt de voornaamste reden is geweest voor de EU om het te implementeren. Maar verder ben ik niet heel erg ingegaan op de andere redenen.

Alexander Castanon (38:09)
Zo je na de automatisering van grenscontrole is er is er ook een hele belangrijke achterliggende reden. Ik weet niet of je weleens intercontinentaal op Schiphol hebt gereisd maar hier wordt je paspoort niet door een douane medewerker gecheckt maar door EGates die ook kijken of het papsoort wel echt is. Daardoor gaat de grenscontrole veel sneller en is de doorloop van reizigers voorpsoediger.

Marleen Hoorn (39:31)
OK, ja, dat is inderdaad nogal belangrijk om misschien even wat meer op in te gaan.

Alexander Castanon (39:37)
Ja, meer ter nuancering dat look-alike fraude tegengaan niet de enige reden is geweest.

Marleen Hoorn (39:46)
ja, ik heb alle onduidelijkheden eigenlijk wel aan jullie gesteld. Dus ik ben gelukkig een stuk wijzer geworden. Dankjewel daarvoor. Vinden jullie het trouwens goed als ik jullie met voor en achternaam. In de scriptie vermeld? Of hebben jullie dat liever niet?

Alexander Castanon (40:52)
Van mij mag het ook. Hartstikke bedankt.

Lonneke Bontje (41:01)
Ja geen probleem, zou je je scriptie ook met ons willen delen?

Marleen Hoorn (41:04)
Marleen? Ja tuurlijk,

Lonneke Bontje (41:16)
Het lijkt mij onwijs leuk om de resultaten terug te zien. En wellicht kunnen wij weer wat van jou leren.

Marleen Hoorn (41:31)
Jazeker, bedankt en werkze nog vandaag

Alexander Castanon (41:35)
Doeg Marleen