



Norwegian University of  
Science and Technology

## ID-fraud mitigation

A proposal of an Eol evaluation system  
operationalizing common objectives in ID  
proofing

**Øyvind Anders Arntzen Toftegaard**

Master in Information Security

Submission date: May 2017

Supervisor:           Bian Yang, IIK

Norwegian University of Science and Technology  
Department of Information Security and Communication Technology



## ABSTRACT

Title:	ID-fraud mitigation - a proposal of an EoI evaluation system operationalizing common objectives in ID proofing	Date: 31.10.17
Participants:	Øyvind A. Arntzen Toftegaard	
Supervisors:	Internal supervisor: Bian Yang	
	External supervisor: Magnar Aukrust	
Keywords:	Evidence of Identity (EoI), ID fraud, ID proofing,	
	ID verification	
Number of pages: 60	Number of appendix: 5	Availability: Public
<p>ID fraud is a serious problem around the world which can result in crimes like economic fraud, human trafficking and terrorism. Many Norwegian organizations has pointed out challenges in performing ID control. This work shows that there are gaps between secure ID proofing and verification systems - and the way EoI is evaluated in Norway today. A national framework for ID proofing and verification has also been requested by Norwegian ID stakeholders.</p> <p>Internationally, there are already several guides and standards available for organizations on ID proofing and verification routines. However, complexity and variation among them can make them hard to interpret and understand, especially by smaller organizations performing ID control.</p> <p>This report proposes an EoI evaluation system operationalizing requirements to EoI in ID proofing and verification processes. The proposed system can be used to assign different EoI appropriate EoI values, allowing combined EoI to be mapped to functional EoI levels. The suggested system is designed to be included in a computer application, allowing easy use by front-desk officers.</p>		

## SAMMENDRAG

Tittel:	Forebygging av ID-relatert kriminalitet – operasjonalisering av vanlige mål for ID-fastsettelse i et EoI evalueringssystem	Dato: 31.10.17
Deltaker:	Øyvind A. Arntzen Toftegaard	
Veiledere:	Intern veileder: Bian Yang	
	Ekstern veileder: Magnar Aukrust	
Stikkord/nøkkelord:	Identitetsbevis (EoI), ID-kriminalitet, ID-fastsettelse ID-verifisering	
Antall sider: 60	Antall vedlegg: 5	Publiseringsavtale inngått: Ja
<p>ID-svindel er et stort problem globalt og kan resultere i kriminalitet som økonomisk svindel, menneskehandel og terrorisme. Mange norske organisasjoner har pekt på utfordringer med å utføre ID kontroll. I tillegg viser dette prosjektet at det er flere sikkerhetshull i dagens norske ID kontroll system. Flere norske organisasjoner involvert med ID-kontroll arbeid har allerede etterlyst et nasjonalt rammeverk for evaluering av ID-bevis.</p> <p>Det finnes allerede mange guider og standarder om ID-evaluering tilgjengelig for organisasjoner som utfører ID-kontroll. Imidlertid kan de ansees som komplekse å forstå og i tillegg varierer innholdet mellom de ulike rammeverkene. Spesielt mindre organisasjoner kan antas å ha utfordringer med tolkning av rammeverkene.</p> <p>Denne rapporten foreslår et EoI-evalueringssystem som operasjonaliserer krav til ID-bevis i forbindelse med ID-kontroll. Det foreslåtte evalueringssystemet kan benyttes for å tildele ulike ID-bevis passende bevis-styrke verdier og bli koblet til funksjonelle EoI nivåer. Det foreslåtte systemet er designet for å bli integrert i et datasystem for å gjøre ID-kontroll prosessen så enkel som mulig for organisasjonenes ansatte.</p>		

## **Preface**

This thesis has a publication ready 12-page Springer-template version attached. The attached short-version focuses on the EoI evaluation system proposal. The main text has the same content, but has in addition dedicated its first part to an extensive analysis of the Norwegian EoI evaluation system including the execution of two real-life fraud attacks.

Writing this thesis as a part-time student has resulted in many late working nights. The good support of internal supervisor Bian Yang and external supervisor Magnar Aukrust has been absolutely necessary and priceless during this period. Special thanks are given to them. Great thanks are also given to all those other people who has supported and believed in this work, being security experts, ID experts, authority employees and more.

Special thanks also to my wife Joyce Mirano for letting me work these many late nights, and taking a big responsibility for keeping our home liveable at this time. I love you so much. Last thanks are sent to my parents Elisabeth Arntzen and Lars Toftegaard for being interested in this work and being helpful with sharing their experiences and knowledge as authors.

## Table of contents

<b><u>PREFACE .....</u></b>	<b><u>3</u></b>
<b><u>1.0 INTRODUCTION .....</u></b>	<b><u>6</u></b>
1.1 BACKGROUND.....	6
1.2 RESEARCH QUESTION AND SCOPE.....	8
1.3 RESEARCH METHODOLOGY .....	8
1.4 ETHICAL CONSIDERATIONS .....	9
1.5 POSSIBLE ERRORS AND LIMITATIONS .....	10
1.6 TERMS .....	11
<b><u>2.0 LITERATURE REVIEW.....</u></b>	<b><u>12</u></b>
2.1 RESEARCH FROM ACADEMIA .....	12
2.2 RESEARCH PROJECTS.....	13
2.3 STANDARDS AND GUIDELINES .....	14
2.4 LEGAL REGULATIONS.....	18
<b><u>3.0 FRAUD ANALYSIS.....</u></b>	<b><u>19</u></b>
3.1 FRAUD METHODOLOGY .....	19
3.2 FRAUD STATISTICS FOR NORWEGIAN ID DOCUMENTS .....	20
3.3 FRAUD EXAMPLES WORLD WIDE .....	21
3.4 FRAUD EXAMPLES FROM NORWAY .....	23
<b><u>4.0 REAL-LIFE FRAUD TESTING .....</u></b>	<b><u>25</u></b>
4.1 GET A PASSPORT ISSUED BASED ON A COUNTERFEIT DRIVING LICENSE ORDERED ON THE DARK WEB (ATTACK A)	25
4.2 GET A PASSPORT ISSUED BASED ON ID DOCUMENTS MAILED TO A FICTIVE ADDRESS (ATTACK B) .....	28
<b><u>5.0 SECURITY ANALYSIS OF COMMON NORWEGIAN EOI .....</u></b>	<b><u>35</u></b>
5.1 REGULAR NORWEGIAN PASSPORT AND THE PASSPORT REGISTRY .....	36
5.2 NORWEGIAN DRIVING LICENSE AND THE DRIVING LICENSE REGISTRY .....	36
5.3 NORWEGIAN BANK CARD AND BANK'S REGISTRIES.....	37
5.4 NORWEGIAN BIRTH CERTIFICATE AND THE NATIONAL REGISTRY.....	38
5.5 NORWEGIAN NATIONAL ID CARD (TO BE LAUNCHED APRIL 2018) AND THE NATIONAL ID CARD REGISTRY.....	39
5.6 SECURITY IN EOI ISSUANCE OR REGISTRATION PROCESSES .....	40
<b><u>6.0 SECURITY GAPS DETECTED THROUGH FRAUD- AND SECURITY ANALYSIS.....</u></b>	<b><u>41</u></b>
6.1 SECURITY GAPS REGARDING ID PROOFING AND VERIFICATION .....	41
6.2 ANALYSIS ON HOW CURRENT FRAMEWORKS MITIGATE GAPS.....	42

**7.0 PROPOSING AN EOI EVALUATION SYSTEM TO IMPROVE ID PROOFING AND VERIFICATION .... 45**

7.1 FINDING EOI VALUES AND USING THEM FOR EOI EVALUATION..... 46

7.2 EOI VALUE REQUIREMENTS FOR ID DOCUMENTS..... 47

7.3 EOI VALUE REQUIREMENTS FOR BINDING TO SUBJECT..... 48

7.4 CALCULATING EOI LEVEL VALUE BASED ON MULTIPLE EVIDENCE AND MULTIPLE BINDINGS TO SUBJECT – A  
METHODOLOGICAL APPROACH..... 49

7.5 MAPPING EOI LEVEL VALUE TO CORRESPONDING EOI LEVELS ..... 50

7.6 THE FULL EOI EVALUATION SYSTEM ..... 51

**8.0 EOI SYSTEMS THAT MIGHT COME IN THE FUTURE ..... 52**

**9.0 DISCUSSION ..... 53**

9.1 FRAUD ANALYSIS ..... 53

9.2 EOI EVALUATION ..... 56

**10.0 CONCLUSION AND REMARKS ..... 59**

**11.0 REFERENCE LIST ..... 61**

**12.0 APPENDIX ..... 67**

12.1 ABBREVIATIONS ..... 67

12.2 LIST OF FIGURES..... 67

12.3 LIST OF TABLES ..... 68

12.4 ADDRESS CHANGE APPLICATION ..... 69

12.5 PUBLISHABLE PAPER DERIVED FROM THIS MASTER THESIS WORK..... 70

## 1.0 Introduction

### 1.1 Background

An identity (ID) document can be used as Evidence of Identity (EoI) in the process of getting access to a service requiring authentication. EoI can be explained as information used to establish or verify a unique identity [1]. According to ISO/IEC 29003 [2], EoI can typically include; I) information provided by the subject, II) issued evidence containing or linking to information about the subject, III) databases and registers containing information about the subject, and IV) information provided by other known sources. Examples on EoI can in other words be a life story, ID documents, public records or registries, social media, personal information like biometrics [3], or a testimony by someone with a relation to the subject. Usually, an ID document has another primary function than being an ID document. Both Passports (travel), driving licenses (driving rights) bank cards (access to funds) and library cards (access to loaning books) are examples on documents giving access to different rights, but which also are able to function as ID documents.

EoI can be required to enrol a subject not previously known to the organization into an ID management system. Such a process can be called ID proofing [2]. EoI can also be required to determine whether a previously enrolled subject is the owner of the claimed identity. This process is often named ID verification. Different ID documents have varying levels of security features. Typically, highly trusted EoI is required to access a high-risk service like for example opening a bank account or having a passport issued. On the other hand, loaning a book at a library can usually be done even with little EoI provided. Requirements to EoI may also differ depending on whether the subject is already enrolled in the organizations system or is applying for access to the service for the first time. Unlawful access to services associated with high risk could result in crimes such as terrorism, economic fraud and human trafficking.

ID fraud is a serious and growing problem around the world. According to the American strategy and research company Javelin, ID fraud hit record high in 2016 with 15,4 million US victims and a cost of \$16 billion [4]. Also in 2016, a fraud indicator report based on research by the University of Portsmouth estimated annual ID fraud losses in the UK could be as much as £5,4 billion [5]. To counter ID related fraud, many nations and international organizations



have developed frameworks in order to standardize ID proofing and verification techniques. Examples on national frameworks are New Zealand's EoI standard related to online services and E-governance [6], Canada's standard on identity and credential assurance [7], UK's national good practice guide on identity proofing and verification of individuals [8], Australia's guide for national identity proofing [9], and Norway's ID establishment guide (only at draft stage) [10]. Examples on global frameworks are the International Civil Aviation Organization's MRTDs – towards better practice in national ID management [11] and the ISO/IEC 29003 standard on identity proofing [2]. In addition, the EU research project ORIGINS [12] has provided recommendations on ID document standardization to the new standardization committee CEN/TC 224 WG 19 [13] established early 2017.

Many Norwegian organizations have described ID proofing as challenging. Examples are the Norwegian Directorate of Immigration [14], the Norwegian Labour and Welfare Administration [15], the Norwegian Tax Administration [16], the Norwegian National Police [17], and the Norwegian ID Centre [18]. Organizations performing ID proofing and verification have to interpret complex content of available frameworks. In addition, available frameworks deviate in content. A consequence could be EoI misjudgment due to content misinterpretations. One real-life example on such misjudgment is the ballot paper for the Norwegian parliamentary election of 2017. It states that any ID document with the holder's name, birth-date and picture can be used to vote [19]. This can allow use of digital ID documents on smartphones, corporation's access cards, and other ID documents which are difficult for election officers to be familiar with [20]. Already in 2013, the Norwegian ID Network, consisting of 14 Norwegian ID stakeholders, pointed out the need of a national ID proofing and verification framework for Norway [21].

Since it is not likely that any front desk officer will be familiar with characteristics of all available EoI, this could be solved by either requiring only ID documents known by the officer, or by requiring combinations of EoI. For the latter case, a computer application could calculate if the combined EoI of the subject provide a sufficient EoI level for access to the service offered by the front desk officer's organization.

## **1.2 Research question and scope**

The objective of this work is to close security gaps within ID proofing and verification by adjusting and simplifying ID proofing and verification processes. To succeed, this project will identify common ID fraud methodologies, analyze the status of ID proofing and verification methodologies, and attempt to adjust the content of these frameworks into a simpler EoI evaluation methodology. The proposed methodology should be possible to insert into a computer program, allowing it to be used by any organization performing ID proofing and verification, regardless of the front desk officer's knowledge.

**Research question:** What are the most severe security gaps of today's Norwegian ID management system and can it be proposed one consistent methodology which Norwegian organizations performing ID control can use for ID evaluation to close these security gaps?

The work in this project will have a focus on the Norwegian EoI system. At the same time, where applicable, results shall be presented in a way that also international organization will be able to use the same principles. The Norwegian national ID card is not yet released, but it will still be included in this evaluation as it will probably enter the market only a few months after this work will be finished.

It is expected by the author that this work will find several security weaknesses in Norway's EoI system. It is also expected by the author that this work will be able to suggest a system to evaluate EoI in a way allowing it to be effectively mapped to different EoI values and/or levels.

## **1.3 Research methodology**

Leedy and Ormrod [22] describes qualitative research as *“looking at characteristics, or qualities, that cannot be entirely reduced to numeral values. A qualitative researcher typically aims to examine the many nuances and complexities of a particular phenomenon”*. Based on this characterisation a qualitative approach would be most suited for this work. A quantitative approach is described by the same authors as *“looking at amounts, or quantities, of one or more variables of interest”*. Such an approach is also partly followed in this work. Starting with a qualitative approach, this paper does not aim to prove a hypothesis right or wrong. Instead both qualitative and quantitative techniques is used on the way to propose a

simple methodology operationalizing common objectives in EoI evaluation. In addition, the best way to fully examine the research question, is assumed by the author to be a presentation of the elements of such an EoI evaluation system ready-to-use. The main methodical structure of this paper is based on recommendations for qualitative studies in [22]. At the same time, this paper also includes quantitative analyses of both security gaps and ID proofing and verification frameworks. Last, the EoI evaluation system proposed in this report is a quantitative system allowing quantitative functionality testing in the future.

This study is based on an extensive literature review, stretching from first data collections in 2015, until last literature searches in 2017. Sources were found based on I) online searches in databases like IEEE Xplore and Springer Link, II) recommendations from meetings with employees of nine Norwegian ID stakeholder organizations, and III) cooperation with the EU-supported ORIGINS project including 15 European ID-stakeholders and research institutions.

While it seems to have been performed quite some research on technical ID management like for example biometrics [23,24,25,26,27], less research seems to have been performed on ID proofing and verification at policy level. Several of the sources used in this report is from newspapers and non-scientific work such as guides and standards. The reason is that such sources can provide information not found in research papers at this point of time. Another research project on EoI evaluation has described the same benefits and need of using such types of sources [28].

#### **1.4 Ethical considerations**

Descriptions of real-life ID-theft attacks performed in this project consists information on how to perform ID-theft in Norway. It might be argued that this report reveals important information which should be subject to a duty of secrecy. At the same time, most parts of the fraud methodologies described in this work are already available online in different webpages [29,30,31]. The author of this project has only put the available methodologies together. It is assumed by the author that fraudsters easily can find the same information and perform the same attacks as described in this work. The author has estimated the value of letting government and other ID-stakeholders know about these vulnerabilities as higher than the cost of eventual ID-fraud committed as a result of reading ID-theft methodology in this

report. The most obvious reason is that criminals will find this information anyway when looking for it.

For the real-life ID-theft tests in this project, the author evaluated the use of a partner to steal the ID of. Use of a such a fellow conspirator were evaluated to be within ethical and legal limits. However, it was decided that the author as long as possible should only steal the author's own identity. The reason was that if any ID-related challenges should occur in the aftermath, it would as much as possible only affect the author. A person with legal background were consulted before and during the real-life ID-theft tests to make sure legal boundaries were not crossed. In addition, security gaps found through the tests were presented at the Norwegian Biometrics Forum in October 2016 [32], giving ID stakeholders approximately a full year to close security gaps pointed out before they were published in this work.

### ***1.5 Possible errors and limitations***

The ID fraud analysis given in this report is mostly based on single tests and sources like news media. It is often single cases in media that have been used. This means that even though security gaps are pointed out, this work does not say much about how frequent or common any exploitation of these gaps are.

Uncertainty in the proposed EoI evaluation system will mostly be connected to which degree correct requirements have been set for EoI evaluation in Table 7.1 and 7.2 of this report. Requirements in the tables are mostly inspired by other nation's guides and standards and knowledge of the author. However, choosing correct requirements is a delicate task. At the same time the introduction of digital ID documents complicates the process of choosing correct requirements, since such ID documents are not covered directly in available guides and standards. Use of main elements from ISO/IEC 29003 [2] does however ensure some level of reliability and validity regarding main principles of EoI evaluation used in this work.

## 1.6 Terms

Definitions used in this report are mainly based on the ISO/IEC 29003 standard on ID proofing [2]. It is used because ISO has a widespread portfolio of standards and it can be assumed the 29003 standard will be used by many parties in practice. Other sources are used where the ISO standard does not provide any definition.

**Identity proofing** – “Process to verify identifying attribute(s) to be entered into an identity management system and to establish that the identifying attributes pertain to the subject to be enrolled” [2].

**Verification** – “A process performed to determine whether the applicant is the owner of the claimed identity” [8].

**Evidence of Identity** – “Evidence that provide a degree of confidence that a subject is represented by the identity being claimed” [2].

**Authoritative Evidence** – “Holds identifying attribute(s) that are managed by an authoritative party” [2].

**Corroborative Evidence** – “Holds identifying attributes that are not managed by an authoritative party” [2].

**Proofing information** – “Information collected for identity proofing” [2].

**Note 1:** Evidence of Identity can be ID documents, document databases, official records, an interview, a guarantor, own knowledge of the applicant, social footprint, biometrics, or a detailed life story [33].

**Note 2:** Authoritative Evidence could be both a corporation controlled database and an official registry. Corroborative Evidence may not be as up-to-date and accurate as Authoritative Evidence [2].

**Note 3:** An authoritative party is an entity that has the recognized right to create or record, and has responsibility to directly manage, an identifying attribute [2].

**Note 4:** Proofing information can be provided by either the subject or a reference [2].

## **2.0 Literature review**

### **2.1 Research from Academia**

In 2004, Mason [34] conducted a survey considering the different forms that make up an identity and in what circumstances identity may be necessary to establish in order to obtain a service. The author claimed that by using paper documents, a fabricated identity can be created overnight. However, attempting to create a false identity with an electronic biographical trail, would according to the author take far longer.

In 2008, Evans-Pughe [35] did a survey exploring how secure our digital identity really is. The history has shown that as more personal data is used and digitally spread, the less value it has because it becomes more available. To follow up security, more and more person-related data are required for authentication purposes. According to the author we need to decide what is an acceptable level of publication of our digital identity.

Another study in 2008, by Agbinya, Islam & Kwok [36], had focus on a digital identity management system. Using artificial neural networks, face recognition and fingerprint recognition, a digital environment identity were developed in .NET and tested. A digital identity management system using multi-modal authentication would according to the authors play a very big role in reducing cases of identity theft and fraud on online services. According to the authors the system was effective in providing the identities of the subjects.

In 2012, The authors Wu et al. [37] proposed a personal identity management cycle model which could capture important events that happened around the management issues of a personal identity. The authors hoped the model might be used to address different issues in identity fraud. In their survey they presented an outline of a lifecycle model in capturing essential events and conditions for a person's identity.

In 2013, Yang et al. [28] investigated the status of EoIs in the scope of ePassport issuance. The authors attempted to define the implementation types, fraud scenarios, security objectives, and trustability levels for EoIs. This had according to the authors not been clearly defined in existing research or in standardization societies so far. In addition, they investigated recommendations from policy and technology perspectives towards highly trusted future ePassport issuance standardization and practice. The authors gave the following

recommendations: I) EoI security deserves more attention, and international standardization efforts should be invested in this field. II) To achieve compatibility with existing EoIs, the security enhancement should to the largest extent be backward compliant, for example through barcode based solutions. III) ePassport issuance authorities should be equipped with cross-reference infrastructure to exploit the identity attributes redundancy between the credential and the identity register records for data corroboration. IV) Multiple EoI databases should be available for data corroboration among each other to ascertain the identity's validity before ePassport issuance. V) Security feature solutions with different levels of trust should be planned for standardization to meet requirements from varied nations or regions. VI) Biometrics can be an effective tool to prevent impersonation based fraud.

## ***2.2 Research projects***

In 2012 the European Commission decided to finance the FIDELITY project [38]. It analysed shortcomings and vulnerabilities in the ePassport life cycle, and provided technical solutions and recommendations to overcome them. Most of the results of this work are however confidential. In 2015, the Commission also decided to fund the ORIGINS project [12]. The ORIGINS project studied security levels of ID documents used in the passport issuance process, and gave recommendations to close security gaps in ID document systems within the EU/Schengen area. This project also resulted in mostly confidential reports.

Dealing with EUs external borders, FRONTEX [39] performed a study from 2010 to 2011 on ePassport security. Objectives of the study were I) to establish an inventory of security relevant issues in the context of the application for, production, and use of ePassports in Europe, II) to find differences among EU/Schengen member States and highlight eventual problems for interoperability when the passports are used for identification at external borders, III) to identify best practices related to the issuance processes, and IV) to suggest a set of recommendations to restore security in the issuance process. The study concluded that reliability of the ePassport issuance process is vital for EU border control. It further concluded that since national ID cards of member states are also accepted as travel documents at the EU/Schengen border, and the security of national ID cards are not standardised, they might be considered as a weak link in border control.

The Organization for Security and Co-operation in Europe (OSCE), arranged a roundtable gathering in 2013 addressing the link between travel document security and population registration/civil registration documents and processes [40]. The aim was to explore the latest trends in forging travel documents, what measures that have been taken to securely identify people in the process of travel document issuance, and what more the OSCE can do to enhance international efforts that link travel document issuing systems to civil registry systems as part of robust national identity management and travel document issuance. Main findings were that; I) secure civil registration systems and documents in many OSCE participating states are central in the travel document issuance process, II) civil registry systems are gaining international significance and determine the level of trust in a country's travel document, III) civil registry upgrades need to go in parallel with travel document upgrades, IV) the international community needs to continue dialogue on the possibility of developing assistance related to the establishment and validation of identity during travel document issuance, V) border control officers need to remain central to travel document inspection, and VI) the variety and number of security features on current travel documents are a "double edged sword" for border control (due to time limitations in checking security features at the border).

### ***2.3 Standards and guidelines***

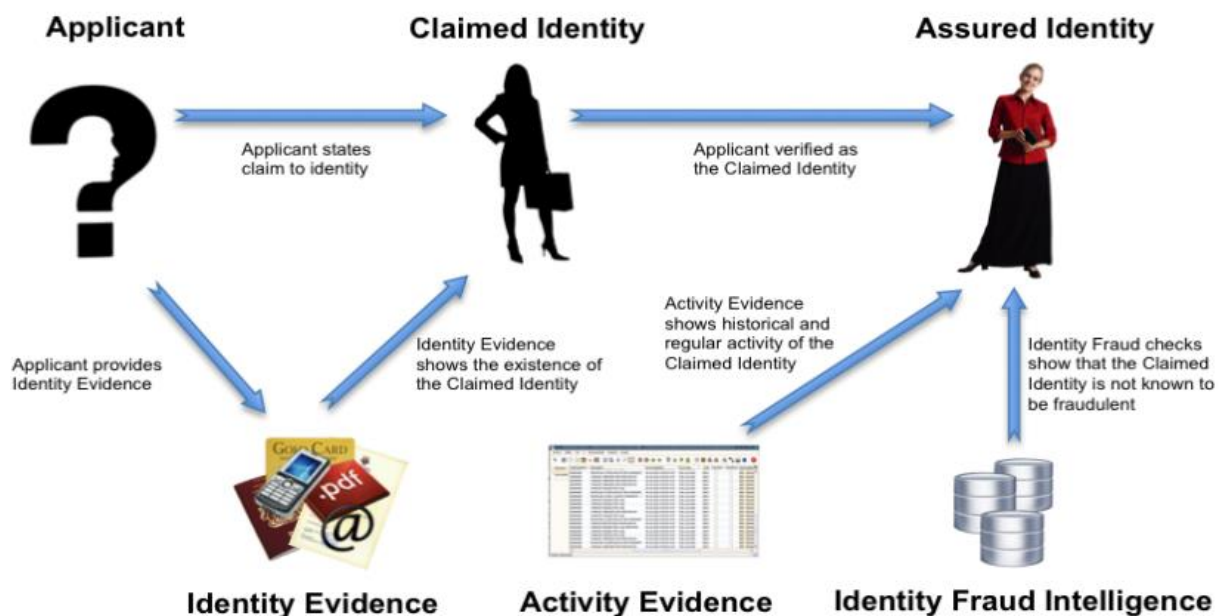
**The Australian Attorney-General's Department** have developed a guide for national identity proofing [9]. The guide states that the backbone of Australia's identity infrastructure is not a single identity card, but rather provided by around 20 government agencies that manage over 50 million core identity documents. The infrastructure is also supported by non-government organizations like banks and universities.

The guide claims that the EoI strength level of a person's identity is established through 5 main identity proofing objectives; I) confirm uniqueness of the identity in the intended context, II) confirm the claimed identity is legitimate, III) confirm the operation of the identity in the community over time, IV) confirm the linkage between the identity and the person claiming the identity, and V) confirm the identity is not known to be used fraudulently.



All these objectives are evaluated using 4 levels of assurance (low, medium, high and very high). The very high level is considered the gold standard and is used for passport issuance. The guide states a variety of requirements to achieve this EoI strength level, including highly trusted governmental ID documents. For those who cannot fulfill the requirements, alternative methods can be used, such as providing multiple less trusted ID documents, or in case of children, verifying the ID of the parents.

The UK's Cabinet Office has issued a good practice guide on ID proofing and verification of individuals [8]. The guide explains that within UK there is no official set of attributes or a single issued document with the primary purpose of identifying an individual. Instead, a combination of different EoI provided, the strength of it, the related verification and validation processes, as well as the activity history, can be used to evaluate the EoI. The UK guide further depicts four levels of identity proofing, where the fourth level includes the use of biometrics to link the examined person to the claimed ID. An example of the ID proofing process can be seen in Figure 2.1. The guide recommends that all these steps are adequately completed.



**Figure 2.1:** Overview of the ID proofing and verification process by the UK's Cabinet Office [8].

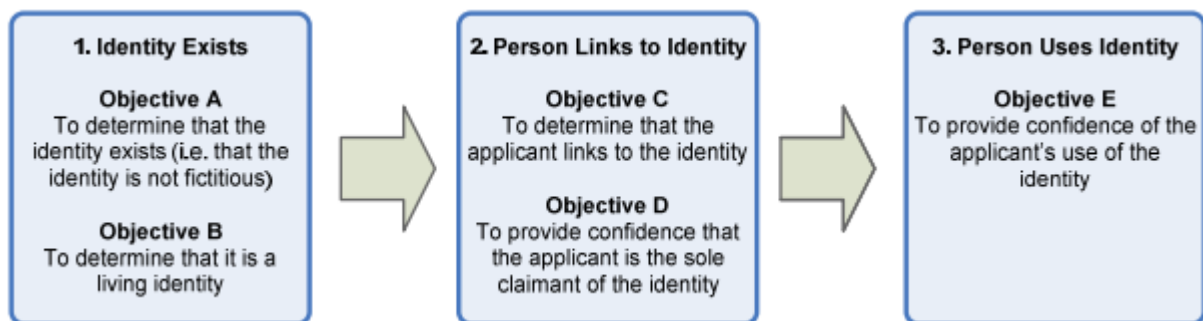
**The New Zealand Department of Internal Affairs** has worked out a national EoI standard related to online services and E-governance [6]. The standard is meant to provide government agencies with good practice guidance about the required process for initial establishment and subsequent confirmation of an individual's ID. It enables agencies to determine the level of risk as low, moderate or high for each of their services, and to identify appropriate EoI requirements. Listed EoI objectives in the standard are; I) ID exists, II) ID is a living ID, III) presenter links to the ID, IV) presenter is sole claimant of the ID, and V) presenter uses the ID in the community.

**The Canadian Treasury Board Secretariat** has presented a standard on ID and credential assurance [7]. The objective with the document is to ensure that ID risk is managed consistently within the government of Canada as well as other jurisdictions and industry sectors. The standard describes four levels of ID assurance: Little confidence, Some confidence, High confidence and Very high confidence. The same levels are connected to credential assurance (confidence level that the individual has maintained control over a credential that has been entrusted to him or her and that the credential has not been compromised. In addition, the standard lists a set of minimum requirements to establish an ID; I) uniqueness, II) EoI, III) accuracy of ID information, and IV) linkage of ID information to individual. EoI in this context are defined by the Secretariat as a record from an authoritative source indicating an individual's ID.

**The Norwegian ID Network** are currently working on a national ID establishment guide. The draft [10] suggest an ID establishment process can be divided into; I) gaining EoI, II) controlling EoI against information about the ID, and III) determining if provided EoI strength level matches EoI requirements of the service applied for. Further, the ID Network divide EoI into; I) information about identity that the person him/herself provides, II) ID document issued by a public or private company, III) written declaration about claimed ID from a reference person with known ID, and/or IV) information about ID from other known sources.

**The International Organization for Standardization** are developing the document ISO/IEC DIS 29003 [2], with the title Information technology – Security techniques – Identity proofing. This up-coming international standard includes guidelines for identity proofing of persons, as well as specifies four levels of identity proofing, and requirements to achieve these levels.

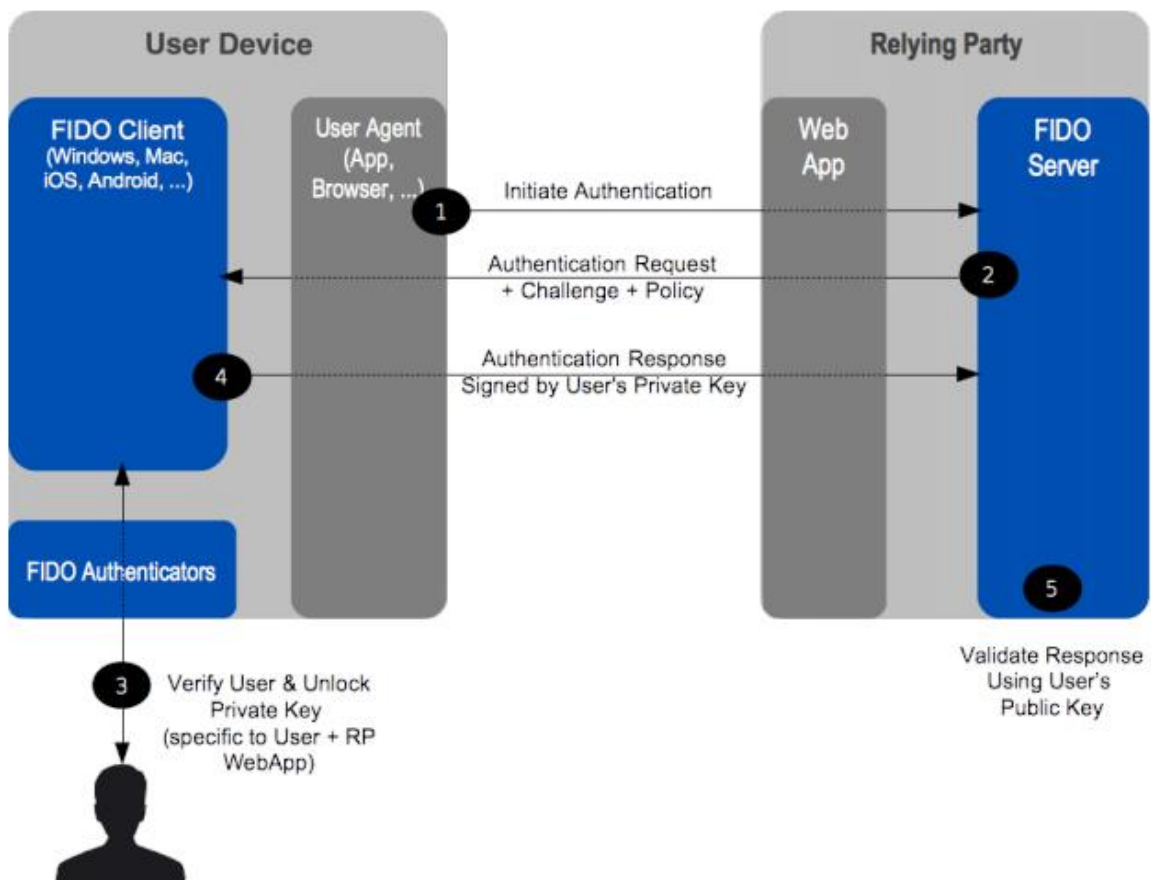
**The International Civil Aviation Organization (ICAO)** has written a guide proposing measures in different areas of interest throughout the travel document issuance process where a high level of confidence may be achieved [11]. The Guide includes three key principles that are central to most EoI frameworks (Figure 2.2). The three principles include a set of EoI objectives to assure confidence in a person's ID prior to issuing a passport; I) ID exists, II) ID is a living ID (not deceased), III) applicant links to the ID, IV) applicant is the sole claimant of the ID (is not using another ID), and V) presenter uses ID in the community.



*Figure 2.2: Key principles that are central to most EoI framework standards [11].*

ICAO has also worked out an international guide for assessing security of handling and issuance of travel documents [33]. The guide recommends best practices to prevent and mitigate security threats at every step of the passport issuance process. Use of risk assessments and audits for achieving best practices is emphasized, as well as the importance that entitlement decisions should not be outsourced. Privacy and protection of data in the application process is also mentioned as important, as well as standardization of routines and application forms related to document issuance. Also, governments are encouraged to always establish that a person's ID is real – for example by checking that the ID actually belong to a living and not deceased person, through crosschecking suggested ID documents.

**The Fast IDentity Online alliance (FIDO)**, has developed a specification document for a universal authentication framework [41]. The framework is designed to enable online services and websites to leverage strong user authentication. It also shall reduce problems associated with creating and remembering many online credentials. The architecture of the framework is pictures in Figure 2.3, which illustrate an authentication process, using for example face image, fingerprint, or voice print. Organizations fulfilling certain security requirements can be certified by FIDO as authenticator at 2 different security levels.



*Figure 2.3: Authentication message flow by the FIDO alliance [41].*

## 2.4 Legal regulations

The European Union **regulation No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)** entered into force in July 2016. The regulation facilitates a mutual approval of each member-states solutions for eID. It covers eSignatures, eSeals/stamps, eTimestamps, secure digital mail and certificate services for webpage authentication [42]. eIDAS defines 3 security levels: low, substantial

and high. The levels are in general connected to the level of confidence in the claimed or asserted ID of a person. The confidence is built with reference to technical specifications, the related standards and procedures, including technical controls, with the purpose to decrease any risk of misuse or alteration of the ID [43].

The European Union **proposal for a regulation on information and communication technology cybersecurity certification** (“Cybersecurity Act”) lays down a framework for European cybersecurity certification to increase trust, cybersecurity and resilience in Europe’s internal market. For certification purposes, it with similarity to eIDAS proposes to use 3 assurance levels: basic, substantial and high. These assurance levels are meant to apply for both ICT products and for services. As ID management becomes more digitalized, this regulation becomes relevant also for this field. To achieve each of the proposed assurance levels, certain criteria laid down in the regulation have to be met [44].

### **3.0 Fraud analysis**

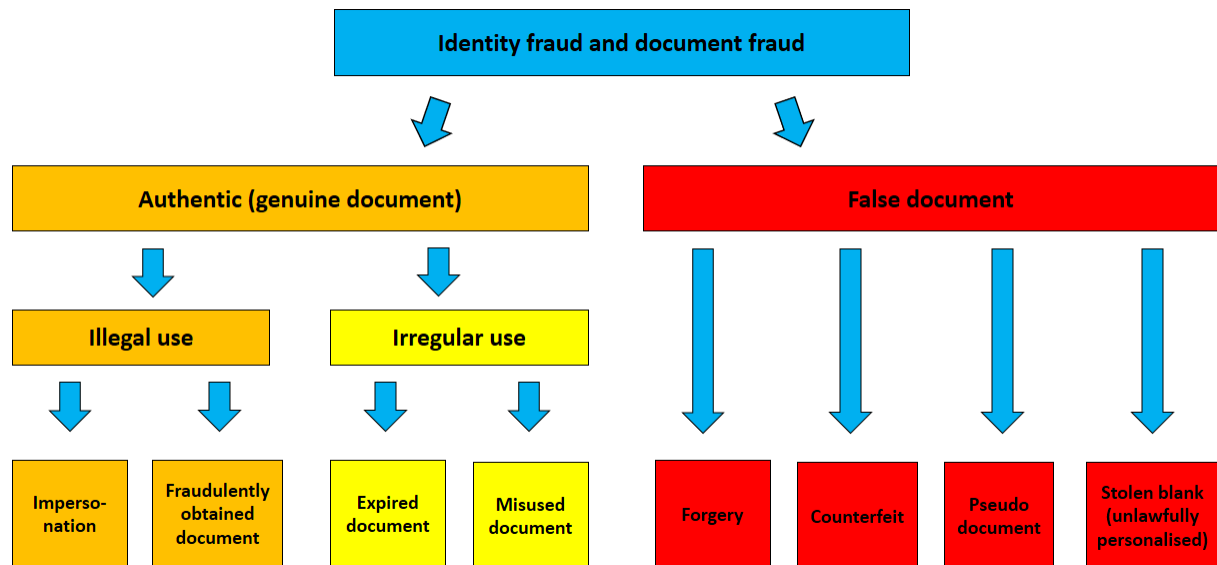
#### ***3.1 Fraud methodology***

ID document fraud can mainly be divided into two categories. The first involves false ID documents, and the second involves genuine ID documents. Fraud involving false ID documents can further be divided into the following sub categories; I) forgery, which involves changes made on a genuine ID document, II) counterfeit, which are full reproductions of original ID documents, III) pseudo, which includes fantasy documents, camouflage documents and similar, and IV) stolen blanks, usually meaning fraudulently obtained genuine documents which are unlawfully personalized.

Fraud by genuine ID documents can mainly be divided into illegal use and irregular use. Illegal use considers; I) impersonation fraud, which means use of an ID document from a legitimate owner with similarities to the fraudulent user, and II) fraudulently obtained ID documents, which relates to use of a dishonest issuing officer or in any other way manipulation of the ID document issuing process in order to obtain a genuine document.

Irregular use might consider ID document misuse or use of expired ID documents. Such acts can be accidental and not deliberate, but it can also be part of illegal use. Irregular use can for

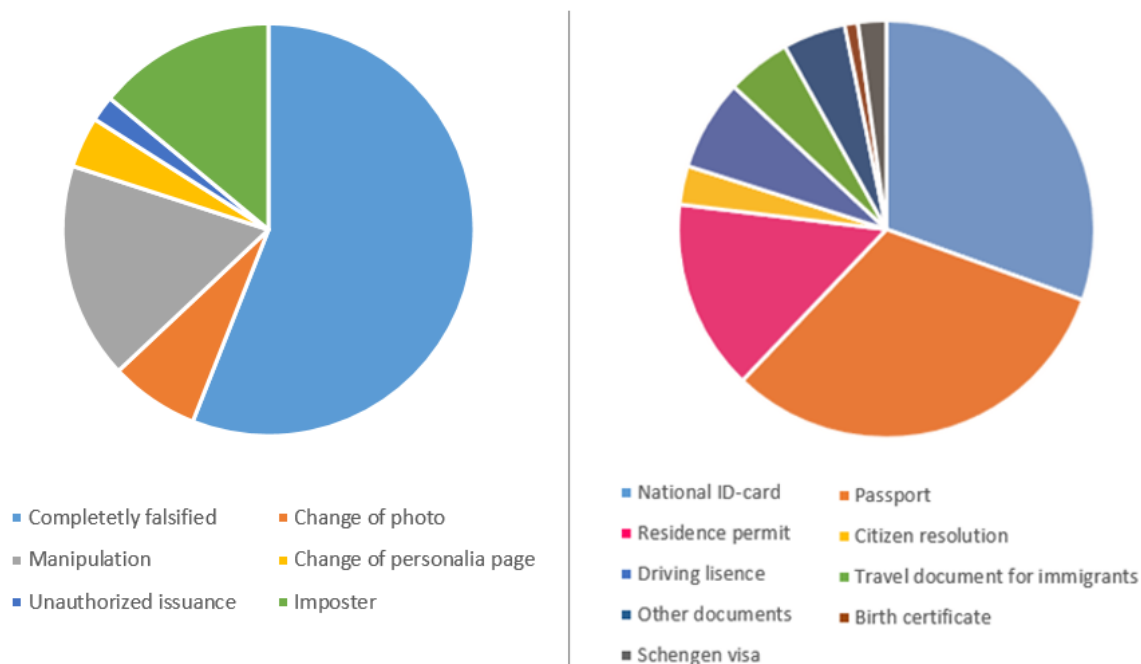
example be combined with false ID documents in relation to fraud. Figure 3.1 gives an overview of all the described ID-document fraud categories [45].



*Figure 3.1: Common fraud methodologies for ID documents [45].*

### **3.2 Fraud statistics for Norwegian ID documents**

In 2015 the Norwegian ID Centre published a report on fraud statistics, showing 866 cases of ID document misuse were reported in Norway during 2014 [46]. This kind of fraud seems to have increased over time, from 678 cases in 2012 and 787 in 2013 [47]. 659 people were caught performing the 787 ID document fraud cases in 2013. That indicates it was common to carry only one fraudulent ID document for each person. Both in 2013 and in 2014, the main country of origin regarding fraudulent ID documents used in Norway, was Italy. Further the statistics showed that during 2014, the largest representation of ID document fraud were completely falsified documents, representing more than 50% of total ID document fraud [46]. On second and third place came document manipulation and imposter documents. Further, passports and national ID cards were first and second regarding types of ID documents most used for fraud. On third place were found residence permit, and on fourth driving license [46] (Figure 3.2).



**Figure 3.2:** Different types of ID document fraud revealed in Norway in 2014 [46,47]. According to the Norwegian ID centre the category “other documents” includes documents like military ID, marriage certificate and transcripts from the National Registry.

### 3.3 Fraud examples world wide

There are many examples of where ID document fraud, mainly through exploiting poor ID proofing, have or probably have been used to commit shady governmental missions as well as serious crimes. Below follows some examples of each.

During the **2010 Dubai assassination of Mahmoud Al-Mabhouh**, 27 assassins - who most of them believed to be members of an elite unit of the Israeli intelligence agency Mossad - arrived the United Arabic Emirates using 12 British passports, 6 Irish passports, 4 French passports, 4 Austrian passports and 1 German passport. The German passport was issued to a “Michael Bodenheimer” by a registration office in Cologne, Germany’s fourth largest city. The passport can be seen in Figure 3.3. By claiming to be from a family of victims from the Nazi regime [48], and providing a marriage certificate of his parents [49], the assumed Israeli agent were able to get issued a German passport. According to the newspaper Der Spiegel, Bodenheimer did not live in Cologne as he had claimed in his application, and no other person by that name lived there at that time either [48], suggesting the identity was fabricated. In this case certain rules of the German constitution were exploited, saying those

persecuted by the Nazis, as well as their children and grandchildren, can petition for repatriation [48].



*Figure 3.3: According to Landytown and Ynet news, the figure shows the passport of “Michael Bodenheimer” [50], and a list of suspected hit squad members [51].*

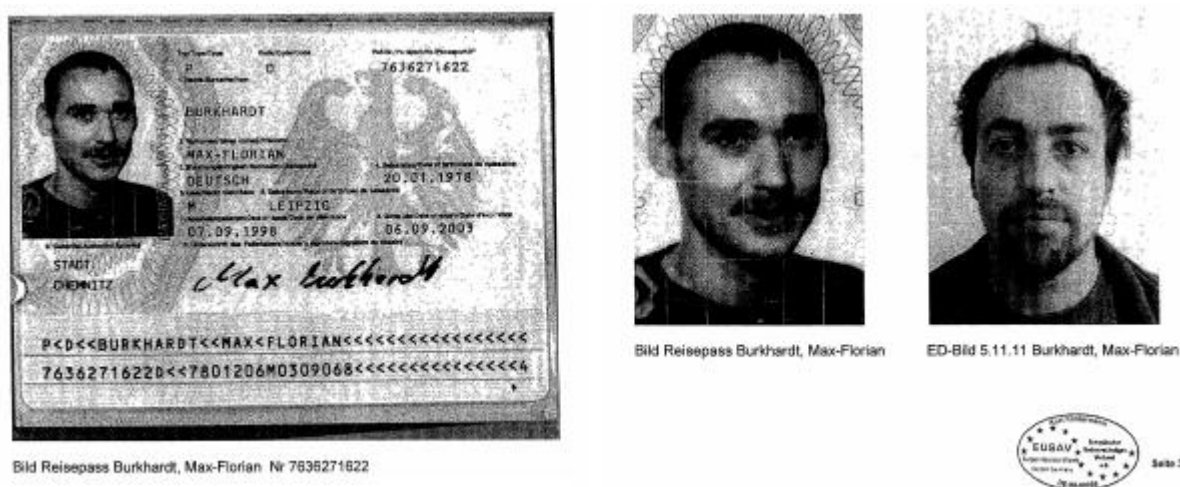
Uwe Mundlos was a member of the German extremist trio forming the **National Socialist Underground**. Preceding his suicide in 2011 he and his two fellow criminals were responsible for 10 extreme right-wing motivated homicides, 2 bomb attacks and at least 15 bank robberies.

While on the run, the trio were hiding for a while in the German town Chemnitz, where they were allowed to stay in an apartment owned by a man named Max-Florian Burkhardt. Max-Florian, with a face looking quite similar to Mundlos, and being approximately of the same height and build, gave Mundlos his ID card and his birth certificate to apply for a passport. Mundlos had passport pictures taken of him and went to a registration office. In 1998, the Chemnitz city government issued a passport that contained the personal data of Max-Florian and a photo of Mundlos [52]. Now there were two persons using the identity of Max-Florian.

The passport and the half-burned birth certificate were later found in the burned-out camper of Uwe Mundlos. Figure 3.4 show the mentioned passport with Max-Florian Burkhardt’s data and the picture of Uwe Mundlos. Uwe Mundlos lived in hiding using the identity of Max Florian Burkard for nearly 13 years (1998 – 2011) [52]. When disappearing in 1998 Mundlos actually did not travel further than 100 km. In addition, the NSU trio went on frequent vacations inside Germany while on the run without getting caught, showing how effective



such impersonating fraud might be, as well as the potential of crimes to get away with over time while living under such a false identity.



**Figure 3.4:** According to NSU leaks, the figure shows the passport of Uwe Mundlos with Max Florian Burkhardt's identity [53].

After **the 2008 Mumbai terrorist attacks**, a Pakistani father and son managing a money transfer agency in Italy were arrested for having sent money - using the stolen ID of another Pakistani man who had never been in Italy and never was involved in the attacks – to activate internet phone accounts used by the attackers and their handlers. The money transfer to a US company gave the attackers five lines over the internet, which were difficult to trace, and allowed the militants to keep in touch, even during the rampage [54].

According to the online encyclopaedia Wikipedia, it was in 2010 revealed a group of ten **Russian agents in the USA**. One of the agents were allegedly using an Irish passport. The passport was issued in the name Eunan Gerard Doherty, to a Richard Murphy (later identified as the Russian Vladimir Guryev). The Russian embassy in Dublin declined to comment the allegations that its officials had used a counterfeit Irish passport. It was later revealed that passports of up to six Irish citizens may have been compromised by the Russian agents. This led to the expulsion of a Dublin-based Russian diplomat in 2011 [55].

### 3.4 Fraud examples from Norway

ID document fraud can be possible in many different ways. One uncommon example is the **data migration error when updating the Norwegian National Registry** in the early

1990ies. The error wrongly registered everyone who migrated from Norway between 1960 and 1975 as Norwegian citizens. The mistake was noticed when several Moroccans showed up at the Norwegian Embassy in Rabat, requiring Norwegian passports [56,57,58].

Another example is the so-called **Passport man** incident, where a story about passport fraud were used to fool the Norwegian Broadcasting Corporation (NRK) as part of a well-planned economic fraud in 2016. A person NRK named the “passport man” claimed to use dishonest servants in the Greek ID document issuing authorities to fraudulent obtain real ID documents for a Norwegian business man. The fictive Greek ID could be used to open bank accounts, get issued bank cards, buy properties, and travel freely in the Schengen area without leaving traces. NRK published the story, but removed it when the scam was revealed [59,60]. It is believed the business man had no involvement with the ID document fraud, but instead was framed by his ex-wife and a previous business partner. That way they could claim in court that he was hiding away money in foreign countries, supported by fabricated ID evidence and NRKs false news-reportage [60].

Another ID fraud example is the **false twins’ social security fraud**. By claiming to have given birth at home to the twins Maxima and Håkon, a Romanian woman living in Oslo managed to milk the social security system for almost 100.000,- Euro between 2003 and 2010 [61]. The method used consisted of a pregnant woman visiting several doctors in other women’s names, getting them registered as pregnant. When the child was born, the child was borrowed to the other women so they could visit health institutions claiming to have given birth at home. This way the child was registered several times, each with a different woman as the mother. The child would in each case get a unique national ID number, triggering supportive payments. In 2013 more than 70 false identities were removed from the Norwegian national registry after a campaign against this type of fraud [62].

A last example can be the **false EEA worker** case, where a carpenter from Armenia managed to acquire seven different Norwegian IDs. Pretending to be an EEA worker, he managed to fraudulently milk the social security system for about 50.000,- Euro. According to NRK, control of ID documents from EEA countries are poorer than for example control of asylum seekers ID documents [63]. EEA ID documents is today assumed by many to be the easiest way for fraudsters into the Norwegian ID system [63,16].

## 4.0 Real-life fraud testing

The following two test scenarios were worked out by the author based on results of the literature review previously described. Passport issuance is used as the final in both tests as passports can be seen as the physical ID document with highest trust in the community and therefore most valuable for people committing ID fraud.

### ***4.1 Get a passport issued based on a counterfeit driving license ordered on the dark web (attack A)***

#### **Background**

Ordering counterfeit Norwegian driving licenses or other ID documents on the dark web, has been described in Norwegian and Swedish newspapers [59,64]. These newspapers give an impression that it is easy to purchase a false ID document online.

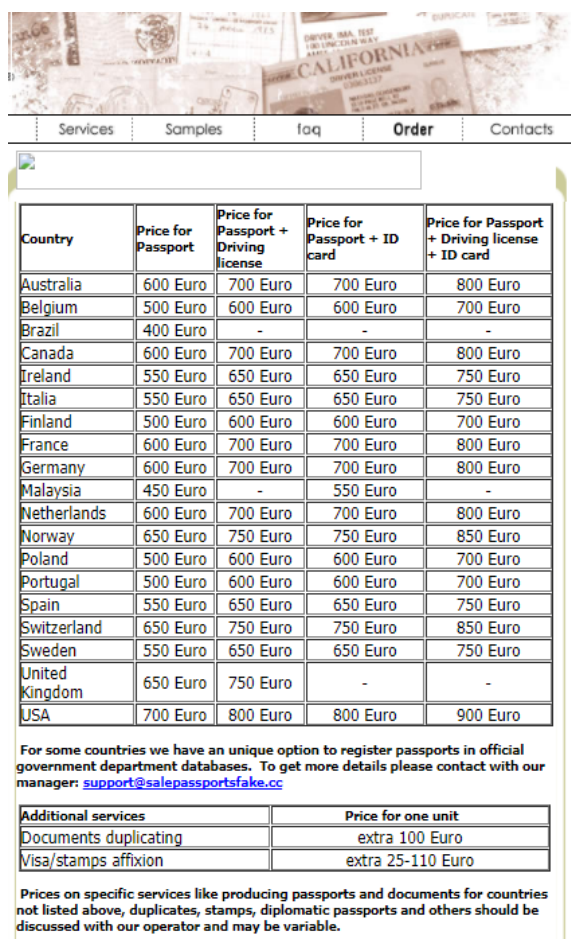
#### **Planned methodology**

- 1) Order a counterfeit Norwegian driving license on the dark web with a picture of the author and fictive biographical information.
- 2) Order a Norwegian driving license from the Norwegian Public Roads Administration including only the same security features as the false license from the dark web. The license should have a picture of the author and biographical information of a fellow conspirator. Then the author shall try to order a passport in the fellow conspirator's name at a Police office. This shall be done by reporting the previous passport as stolen and using the "counterfeit" ID document from the Road Administration.

**Note:** The reason for using a driving license "counterfeited" by the Road Administration in step B, is to avoid transferring any biographical information concerning the fellow conspirator to a criminal ID document supplier in step A.

## Execution step 1

The author ordered a Norwegian driving license from at a fraudulent supplier's webpage [65] mentioned in the media [59,64]. The order was placed anonymously through an unverified email account using the TOR (dark web) browser. The supplier's email address was displayed on the webpage as seen in Figure 4.1.



**SalePassportsFake.cc Order Form**

By placing your order, you must have read and agreed to our [Terms of Service](#).

The order procedure is the following:

1. You send us all the necessary information (depending on the document you want to order). We receive and process your order and give you payment information.
2. You pay 25% upfront money as prepayment for document(s) producing.
3. We start to produce your document(s). Time constraints are 2-5 days (depending on your order).
4. We send you scan/photos of your ready-made document(s). You check all the details and give us confirmation.
5. You send us the rest of full amount and your delivery address. You will receive your document(s) in several days via UPS, FedEx or DHL (free of charge for you).

We accept following payment method:

1. Western Union ([westernunion.com](http://westernunion.com))  
Western Union is a global leader in money transfer and message services, with a history of pioneering service dating back more than 150 years. Western Union continues today to help consumers and businesses transfer money or make payments using money orders and other electronic systems. Consumers can quickly and easily transfer money to more than 170,000 Western Union Agent locations in over 190 countries worldwide - the largest network of its kind. Western Union also markets more than one quarter billion money orders every year. With about \$3 billion in revenue, Western Union remains an industry leader with an eye toward providing fast and reliable money and messaging services. Australia, Austria, Canada, France, Germany, Ireland, Italy, Netherlands, New Zealand, Norway, Sweden, United Kingdom and United States citizens can pay online using a Visa or MasterCard credit or debit card.
2. MoneyGram ([www.moneygram.com](http://www.moneygram.com))  
MoneyGram is a global leader in international money transfers and Travelers Express is the largest processor of money orders in the U.S. Together we are two trusted names making up MoneyGram International, Inc. We have helped people and businesses by providing affordable, reliable and convenient payment services since 1940.
3. Bitcoin ([www.bitcoin.org](http://www.bitcoin.org))  
Bitcoin is an anonymous decentralized digital currency that enables instant payments to anyone, anywhere in the world. It's the first practical implementation of a cryptocurrency, a form of money that uses cryptography to control its creation and management, rather than relying on central authorities.

To get the additional information and place the order mail us: [support@salepassportsfake.cc](mailto:support@salepassportsfake.cc)

You can find all necessary information to place an order for passport below:

- Your surname:
- Your given names:
- Your sex (M or F):
- Your date of birth:
- Your place of birth (city and country):
- Your passport number (optional):
- Date of issue (optional):
- Issuing authority (optional):
- Your address (optional):

Country	Price for Passport	Price for Passport + Driving license	Price for Passport + ID card	Price for Passport + Driving license + ID card
Australia	600 Euro	700 Euro	700 Euro	800 Euro
Belgium	500 Euro	600 Euro	600 Euro	700 Euro
Brazil	400 Euro	-	-	-
Canada	600 Euro	700 Euro	700 Euro	800 Euro
Ireland	550 Euro	650 Euro	650 Euro	750 Euro
Italia	550 Euro	650 Euro	650 Euro	750 Euro
Finland	500 Euro	600 Euro	600 Euro	700 Euro
France	600 Euro	700 Euro	700 Euro	800 Euro
Germany	600 Euro	700 Euro	700 Euro	800 Euro
Malaysia	450 Euro	-	550 Euro	-
Netherlands	600 Euro	700 Euro	700 Euro	800 Euro
Norway	650 Euro	750 Euro	750 Euro	850 Euro
Poland	500 Euro	600 Euro	600 Euro	700 Euro
Portugal	500 Euro	600 Euro	600 Euro	700 Euro
Spain	550 Euro	650 Euro	650 Euro	750 Euro
Switzerland	650 Euro	750 Euro	750 Euro	850 Euro
Sweden	550 Euro	650 Euro	650 Euro	750 Euro
United Kingdom	650 Euro	750 Euro	-	-
USA	700 Euro	800 Euro	800 Euro	900 Euro

For some countries we have a unique option to register passports in official government department databases. To get more details please contact with our manager: [support@salepassportsfake.cc](mailto:support@salepassportsfake.cc)

Additional services	Price for one unit
Documents duplicating	extra 100 Euro
Visa/stamps affixion	extra 25-110 Euro

Prices on specific services like producing passports and documents for countries not listed above, duplicates, stamps, diplomatic passports and others should be discussed with our operator and may be variable.

Figure 4.1: Website offering falsified ID documents on the web [65].

The supplier confirmed the order the next day and asked for a deposit of 25% of the price amount. The author suggested to use a deposit service for secure online payment, to make sure the product would be delivered before the money were transferred to the supplier. The supplier declined this suggestion. As a second option the author suggested to meet at any international airport to make the exchange of money against the ID document. The supplier declined this possibility as well.

The pricelist as can be seen in figure 4.1 show that 25% of the total price is a significant amount of money. For example € 125,- for a Belgian passport. The lack of any warranty that the buyer will receive anything, leaves purchasing an ID document at such an online store an option for desperate or less thoughtful people only. The risk of being scammed is very high. By browsing forums for experiences of online buyers of ID documents, it seems many of these people trying to buy ID documents online have been scammed [66,67].

According to the forums the methodology of scammers posing as counterfeit ID document suppliers is usually to ask for a deposit or payment up front, and after the buyer has paid he or she will never hear from the scammer again. Another methodology described is to ask the buyer for a small deposit first, and keep the contact with the customer to create more trust. Later, the supplier will show the buyer pictures of ID documents with the customers chosen biographic information, and the customer is asked to pay the rest of the amount to have the finished document(s) sent by mail. After the customer pay the rest of the amount, the contact will cease, and no ID document will be received by the customer. It is speculated in forums that the ID documents were created in Photoshop or a similar program only. This further gives reason to believe such webpages is mainly used to fool people, and there is a great chance the real ID document sales market is instead somewhere else. For example in real life or in trusted dark web chat rooms.

## **Execution step 2**

At this point the author decided to terminate test A based on I) it was not found any possibility to purchase a falsified driving license without incredible risk of losing huge amounts of money, II) the author had limited time resources, and did not have time to look further for closed chatting groups or physical market places of falsified ID documents, and III) since the author had no sample model for the Public Road Administration to make a falsified driving license from, the motivation for continuing with this in order to test the passport issuance routines of the Police were reduced. Test of passport issuance was instead intended to be postponed to the next test - attack B.

## **4.2 Get a passport issued based on ID documents mailed to a fictive address (attack B)**

### **Background**

Newspapers have reported that scammers have installed mailboxes in fictive addresses for real-person victims [30]. This show it is possible to change the victim's address to fictive mailboxes and have important mail sent to these without the victim's knowledge.

Authentication by the use of a national ID number is needed to perform such a mail address change. Klingsheim [29] has previously showed that a Norwegian national ID number can be found in an online guessing attack within a few minutes. With control of the victim's mail box and also the national ID number, it is assumed that ID documents can be ordered by a scammer in order to steal the ID of the victim in an impersonating type attack.

### **Planned methodology**

1) Performing a guessing attack on the authors national ID number and order an address change to a new mailbox installed by the author. Then, order new real ID documents (birth certificate, bank card and so on) to the new mail box.

2) Loan ID documents from a fellow conspirator corresponding to the ID documents successfully received to the mailbox. Then use these ID documents in an attempt to order a passport at a Police office, using the imposter method and reporting the previous Passport as stolen.

**Note:** The link between step 1 and 2 is that if the author can create a fictive address for himself and get sent ID documents there, he can also do this for other persons. However, by doing it this way the fellow conspirator will be less involved and has a lower risk of any discomfort, since the author do not have to imposter him at the earliest steps.

### **Execution step 1**

The author successfully guessed his national ID number, changed his address and ordered and received the following ID documents: Birth certificate, residence certificate, marriage

certificate, bank card (without portrait) as well as MinID and BankID eID access. The methodology is described more into detail in the following subchapters.

### ***Guessing national ID number***

A national ID number can be discovered through a guessing type attack [29]. The attacker has to know the victim's name and birth-date before the attack can be launched. Such information can often be found in web pages like facebook. Facebook also usually include a portrait of the profile holder, which can be checked by the scammer in case it is desired to make an imposter attack.

The national ID number consists of 11 characters, where the first 6 are the date of birth. The 7<sup>th</sup> and 8<sup>th</sup> number is given based on what group of years the individual is born. The 9<sup>th</sup> number is referring to sex and will be an odd number if the sex is male and even number if the sex is female [68]. The last two numbers (10<sup>th</sup> and 11<sup>th</sup>) are control numbers ( $k$ ) that can be calculated based on the previous numbers using the following algorithms available online [69]:

$$k_1 = 11 - ((3 * d_1 + 7 * d_2 + 6 * m_1 + 1 * m_2 + 8 * y_1 + 9 * y_2 + 4 * i_1 + 5 * i_2 + 2 * i_3) \bmod 11) \quad (1)$$

$$k_2 = 11 - ((5 * d_1 + 4 * d_2 + 3 * m_1 + 2 * m_2 + 7 * y_1 + 6 * y_2 + 5 * i_1 + 4 * i_2 + 3 * i_3 + 2 * k_1) \bmod 11) \quad (2)$$

In the algorithms  $d$  = day,  $m$  = month,  $y$  = year and  $i$  = individual number. To demonstrate the concept, a date of birth could be 21.01.1983. That gives 210183 as the first 6 characters. The next 3 numbers have to be between 000 and 499 since those were used between 1900 and 1999, or 900 and 999 since those were used between 1940 and 1999 [68]. That gives 000-499 and 900-999 = 600 numbers. Those 600 can be divided by two because the owner of the number is either male or female and therefore only numbers ending with one odd or even number needs to be considered. That leaves only 300 individual numbers to be tested in the guessing attack. If the attacker is low-tech, the numbers can be tried manually in a tele-

company's web-pages. However, by using a custom script, these possible numbers can easily be run through a web page in an automatic way to save time.

Since a user only must provide name and national ID number to order a phone number, and tele-companies want to make a credit check of the person before approving the customer, it is possible to exploit tele-company's webpages for this kind of attacks. If the typed national ID number is wrong, an error message will be given along with a possibility to try again. The author has not found any limit in amounts of tries. However, if any company has such a limit, there are plenty of other tele-companies to choose between.

The author of this project tested the algorithms above on his own national ID number, and found the calculations to be correct. When the correct national ID number is found at the tele-company's web-page, the owner of the ID number will get a notification by mail that someone has made a credit check on him or her. However, to what extent people are reacting to such a credit check notice is unknown.

### *Address change*

The Norwegian Tax Administration has registered two addresses for any person with residence in Norway. One residence address and one mail address (they can be the same address). The Tax Administration allows change of mail address through the use of an address change form sent by regular mail. The form includes the applicant's name, address and national ID number. A copy of a passport, driving license, or other ID document which includes birth-date, signature and picture must be attached to the address change form. It is assumed to be quite easy to either take an unnoticed photo of such a document from any place someone would keep it, or just to falsify data on such a document in programs like Photoshop. This allows address change without having an actual ID document, and by using traditional mail it will not be performed a true authentication of the person asking for the address change.

In this test, it was used a bad scan of a real driving license. It is assumed such a scan could easily be created in Photoshop. The address change form was written by the right-handed author, and signed by a left-handed helper. This document including the scan of the driving license can be seen in Appendix 12.4. The email address was created in a mail service which does not authenticate the subscriber. This allows anyone to be the owner of the email address,



especially if the TOR (dark web) browser is used to create the account. The phone number used was real, but there were no phone calls or messages received regarding the address change, so here a phone number found in a public phonebook could be used safely. The author logged into the public services webpage Altinn a few days later and could see that the address had certainly been changed.

The author at the same time installed a mailbox at a chosen external address (Figure 4.2). The mailbox had the name of the author written on it. Neither the building administration nor the neighbours were told about the experiment, so they had the chance to remove the mailbox if they would discover that it did not belong there. The mailbox was not removed and the author did not receive any comments about it over a time period of two weeks.

The author also asked a post officer on service delivering mail, if she would put an addressed letter in a mailbox somewhere even if it was an additional mailbox looking out of place. She said yes and said there are many places where there are extra mailboxes looking like they don't belong there, but as long as the mailbox matches the address on the letter, the letter will be delivered in this mailbox no questions asked.



**Figure 4.2:** Hallway where the new mail box was installed. 1) Before mailbox is installed. 2) After mailbox is installed.

### ***Birth certificate***

It is not possible to order a birth certificate from the Tax Administration online without using an authentication method like BankID or MinID. To circumvent this, the author called the Tax Administration and ordered a birth certificate by phone. This was possible by providing the national ID number. The operator said the birth certificate would be sent the next day. As a security precaution, it could only be sent to the address registered in the National Registry.

Although previously changing the address in the National Registry, the birth certificate did still not arrive in the new mailbox. After another phone call to the Tax Administration, the author discovered the reason was that the address had not been changed at the Postal Service equally to the address in the National Registry. The address change at the Postal Service was however possible to do over phone by providing the national ID number as authentication only. After the address change at the Postal Service, the birth certificate arrived at the new mail address. Neither the Tax Office nor the Postal Service sent any notification to the old address, or to the address owners phone or email, to notify that the address had been changed.

During the phone-call with the Postal Service, the operator said they do not allow changing mail address over phone unless it matches the address registered in the National Registry. The only possibility to change mail address at the Postal Service to another address than the one registered in the National Registry is to either use an eID like BankID or MinID, or showing up in a postal office with an ID document. This means the easiest way to get a fictive address is to change the address at the Tax Administration by using a picture or scan of an ID document as described above.

### ***Residence certificate***

The author called the Tax Administration again to order a residence certificate. The operator said it was preferred that the certificate was ordered online by use of MinID or BankID, but since the phone conversation was already started, the author was allowed to make the order anyway. The operator asked if it was correct that postal address and residence address was different addresses. The author answered yes to that, and the residence certificate was successfully received a few days later. Note again that there are three addresses in use; I) resident address by the Tax Office, II) mail address by the Tax Office, and III) mail address by the Postal Service. In this test, the mail address by the Tax Office matched the mail address by the Postal Service, which was enough to receive the important mail at the fictive address.

### ***Marriage certificate***

The author got married during the time these fraud-tests were performed. The marriage certificate from the actual marriage was one of the documents received to the mailbox at the fictive address.

***Driving license***

The author tried to order a new driving license from the Road Administration over phone. However, this could not be successfully executed. The operator explained it was a demand that applicants show up at a Road Administration office in person in order to have issued a new driving license.

***Bank card***

Ordering a bank card could be successfully done over phone by providing the national ID number. The operator did however ask a few questions about what happened with the old bank card, where the author explained it was lost on a mountain trip. As a deviation from the author's plan, the bank card was by default sent as a bank card without portrait. This means this bank card is not approved as EoI by many service providers, like for example the Postal Service, or for voting in government elections.

***MinID eID access***

MinID is today the only highly trusted eID in Norway which is free or does not require opening a bank account. It can be used to access tax information and a lot of other social and public online services. The author entered the eID webpage of the Agency for Public Management and eGovernment [70] where the only thing needed to open the MinID account, was the national ID number. After typing the national ID number, the author got a message that log-in codes were on the way to his mail address registered in the National Registry. The codes were received a few days later.

***BankID eID access***

BankID is the highest trusted eID available today for regular private individuals in Norway and gives access to the most protected public services and many private services offered online, with finances being an obvious example. To order this authentication service for the first time, the user must have been through the authentication process connected to opening a bank account. It was however assumed here that the attacker knew the victim's bank. The author therefore called his bank and claimed he had lost his BankID password generator. By providing the national ID number over phone, a new BankID password generator was sent to the author's mail address registered in the National Registry. It was received a few days later.

A BankID password generator alone does not give access to bank accounts or other services. To be able to gain such access, there is a personal password only known to the user that should be typed in as well. There are however two possibilities to get this password; I) to buy profiles with general passwords on the dark web from webpages offering such services (usually based on hacking activity), or II) to get a new password from the bank (by pretending to have forgotten the old password). Option II appears to be the easiest possibility, but the method has not been tried in real-life by the author. To obtain a new password, the related bank must be contacted. According to Difi [71], the bank will then send a new password for BankID to the owner's pre-registered email, and also send a notice to the owner's registered phone number. However, as probably both email address and phone number can be changed through a phone-call to the bank using national ID number as EoI, these measures are probably not sufficient. At the bank Nordea's web pages, the email and phone number can even be changed in a web browser during the password restore process without authentication, triggering a new password to be sent to the mail address registered in the National Registry [72].

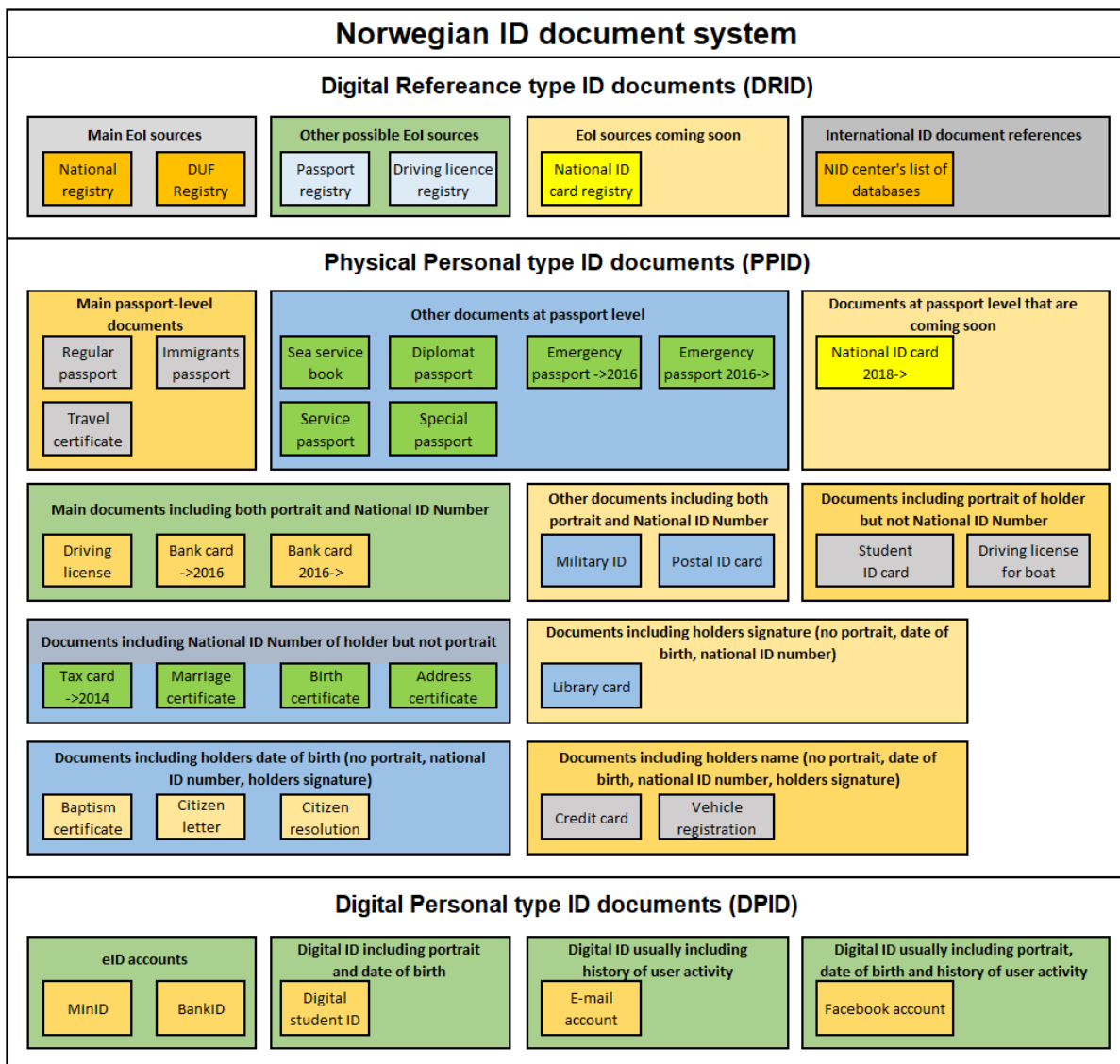
## **Execution step 2**

Documents the author could use in an attempt to get issued a passport in someone else's name would be the following: Birth certificate, Residence certificate, Marriage certificate and a bank card without portrait. In addition, the author could collect life history and family related information of the "victim" in social media and by the use of online public services accessed by MinID or BankID.

The author made several attempts to make an agreement with the Police on a passport fraud test. Personnel on several levels in the passport issuing office in Oslo as well as personnel at national level with responsibility for passport issuance were contacted over a time period of 6 months. Although answers were mostly positive, no one seemed to be in the position of actually being able to allow a passport issuance fraud test. To try having a passport issued in another person's name without the approval of the Police would be on the edge of legal regulations, even with a consent from a fellow conspirator. Therefore, test 2 was terminated at this point.

## 5.0 Security analysis of common Norwegian EoI

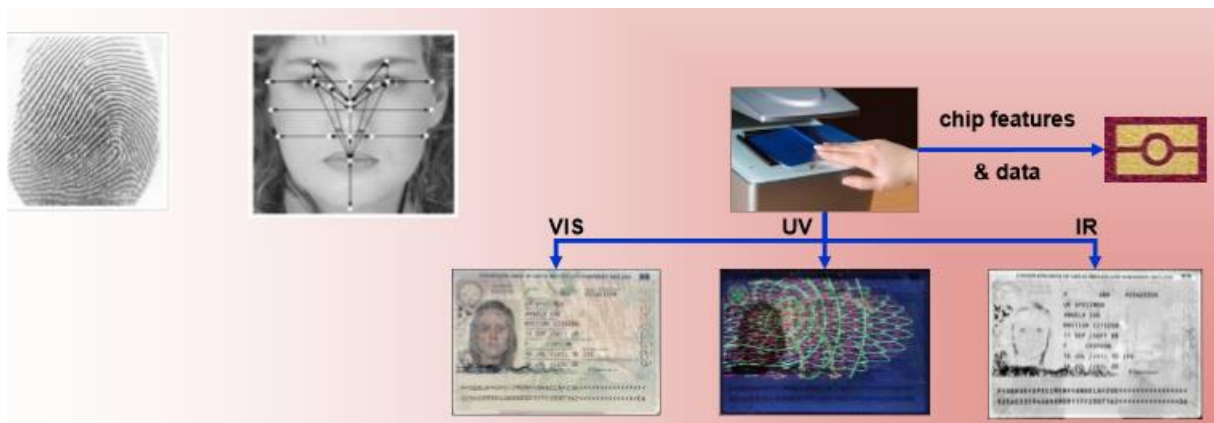
In this chapter security related information will be reviewed concerning the four most common EoIs in Norway, in addition to the coming National ID Card. The information gives a platform for evaluating weak links in the Norwegian EoI system, whether it is technical security features, issuing routines, or other issues. Figure 5.1 shows an overview of commonly used Norwegian ID documents.



**Figure 5.1:** Overview of commonly used Norwegian ID documents. The overview was developed as part of this project. Colours are used for visualization only and have no function. Year illustrate when a new version came and an old version was phased out.

### 5.1 Regular Norwegian passport and the passport registry

A physical inspection of a Norwegian ePassport shows it include data like name, nationality, hight, national ID number, sex, place of birth, the passport issuing authority, date of issuance, date of expiry, signature, portrait and fingerprint of holder. ePassports are currently produced globally at a security level making forgery difficult. As visualized in Figure 5.2, an ePassport specified by the International Civil Aviation Organization in document 9303 [73] contains both visible and invisible security features including ultraviolet, visual and infrared. Globally it also has an embedded RFID chip which contains biometric data in form of face image (mandatory) and fingerprint or iris images (optional). Norwegian passport holders are registered in the Norwegian Passport Registry. The registered information might at least include name, national ID number, signature, height, hair colour, place of birth, and the address where the passport was sent [74]. Additional information can also be registered, typically face photo and signature. The Passport Registry is controlled by the Norwegian National Police and access is governed through the Norwegian passport law and the personal data act. For example might a police officer working with traffic control not have access to the Passport Registry.

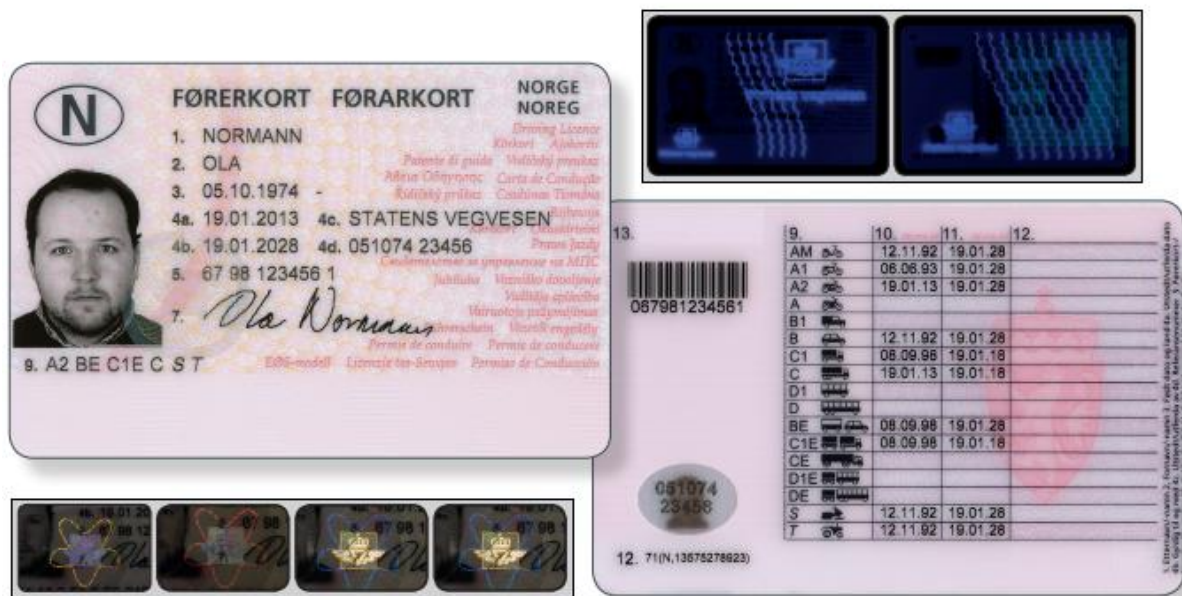


**Figure 5.2:** An ePassport specified by ICAO's document 9303 contains both visible and invisible security features. It also has an embedded RFID chip, which contains biometric data like face, fingerprint and iris images [75].

### 5.2 Norwegian driving license and the driving license registry

Driving license's security features (Figure 5.3) includes high quality text print, security base print, holographic print, relief-pattern, micro print, a black line, wave formed relief text, UV

print, and IR features [76,77,78]. Information on the license contains name, nationality, license number, national ID number, vehicle class(es), license issuing authority, date of issuance, validity time, holders signature and portrait [78]. Driving license holders are registered in the Driving License Registry. The Driving License Registry is managed by the Norwegian Public Roads Administration and content might at least include holders name, place of birth, civil status, national ID number, address, phone number, email address and whether the person is alive or deceased [79].



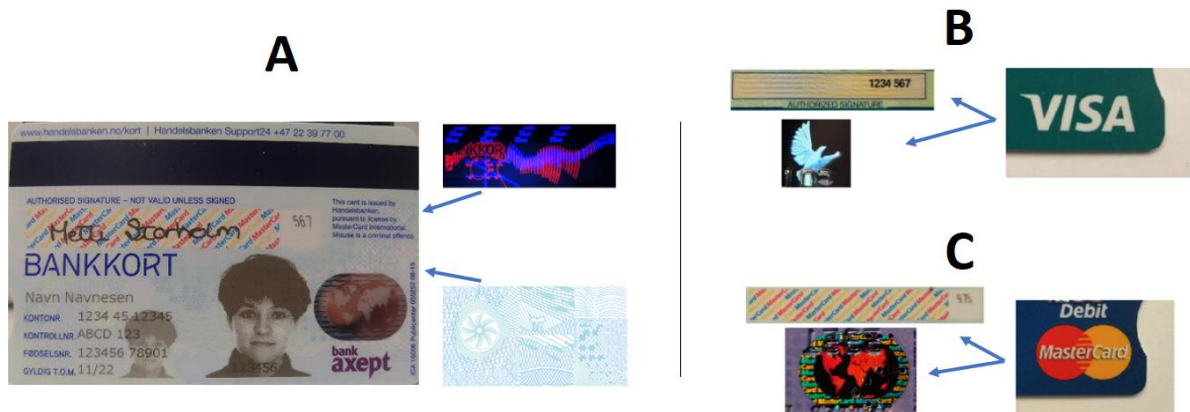
**Figure 5.3:** A driving license with UV light in the upper right corner and holograms in the lower left corner [76].

### 5.3 Norwegian bank card and bank's registries

Bank cards (Figure 5.4) include security features like ink reacting on UV light, micro-text and micropatterns. For Visa cards, the word “Visa” is printed on the front side and there is a dove hologram and a signature field on the backside. For MasterCard there is a MasterCard logo on the frontside and a world map hologram and a signature field on the backside. Norwegian bank card security features are normally either used alone with a BankAxept logo and signature field, or combined with Visa or Mastercard security features [80]. Visual inspection show that a bank card contains information like name, account number, card number, national ID number, control numbers, date of expiry, signature and portrait of



holder. A new trend is that banks prefer to issue bank cards without ID elements like portrait and national ID number, making its value as ID document much lower. Bank card holders are normally registered in registries accessible by the bank company only.



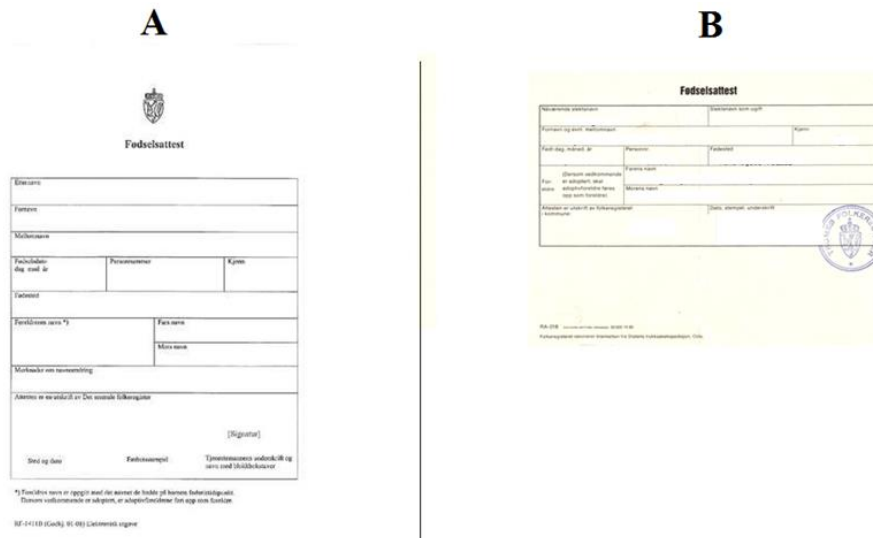
**Figure 5.4:** A) Norwegian bank card with UV and micro features. B) Visa card with dove hologram and signature field. C) MasterCard with world map hologram and signature field [80].

#### 5.4 Norwegian birth certificate and the National Registry

Norwegian birth certificates (Figure 5.5) include security features like a stamp from the issuing authority office, and the officers signature. The birth certificate might contain information like name, sex, national ID number, place of birth, fathers full name, mothers full name, date of issue and municipality of the issuing authority. Birth certificates unlike passports, driving licenses and bank cards, do never expire. The assassin case from Germany referred to in this report's chapter 3.3 shows that ID documents at this level (in that case a marriage certificate) can be used even after death as EoI by children or grandchildren [51]. There is a possibility that something similar could happen in Norway based on the Citizenship Act's rule 19 about exemption from regular requirements in certain citizenship cases [81]. Both marriage and birth certificates are issued by the Norwegian National Registry. The National Registry is managed by the Tax Administration and forms the basis for the Tax Register, the Electoral Register and Population Statistics. The National Registry can be seen as the origin for EoI of Norwegian residents, and it is mandatory for Norwegian residents to be registered there. Stored information might at least include births, names, paternity and parental responsibility, changes of address, changes in marital status, deaths,



name changes, citizenship and national ID number [82]. With this amount of biographic information, the National Registry is commonly used as core source in passport issuance and access to other important services.



**Figure 5.5:** A) Norwegian birth certificate from around 2014 (blank). B) Norwegian birth certificate from 1982 (text and signature removed). Both are printed on regular paper and use signature and stamp as only security features.

### 5.5 Norwegian national ID card (to be launched April 2018) and the national ID card registry

The Norwegian national ID card (Figure 5.6) is estimated to enter the market in April 2018. It will be an international ID document which can be voluntarily purchased by Norwegian citizens. It might also be used as a travel document inside Schengen. The ID document will probably contain information like name, sex, national ID number, nationality, height, signature, portrait and fingerprint [83]. Security features for the national ID card is not known at this point of time. The National ID Card Registry will be managed by the Norwegian National Police. At this point of time, exactly what content will be entered into the National ID Card Registry is not known.



**Figure 5.6:** Winner of design competition for Norwegian ID Card. Final design might however deviate from the picture [84]

## 5.6 Security in EoI issuance or registration processes

Based on associated trust in the community, passports can be seen as the ultimate personal ID document while a registration in the National Registry can be seen as the ultimate EoI. Further, when the Norwegian national ID card will be introduced, it will contain what can be seen as the ultimate eID evidence.

The issuance routines of the new national ID card are not yet known. However, it is assumed it will be quite similar to the passport issuance process of today. The only mandatory EoI required to have a passport issued today is a registration in the National Registry. However, the Norwegian National Police will ask the applicant – if possible - to provide an ID document including the national ID number and a portrait when applying [85]. Such documents are typically the expired passport, a driving license or a bank card. However, the Police have to approve a less trusted document to establish the ID for people who does not have these ID documents. In order to reduce risk, for example parents of an applicant who can only provide less trusted ID documents (for example birth certificate), can be asked to show a higher trusted ID document and confirm the claimed ID. This is already routine by the Police [85].

A registration in the National Registry is normally based on either a notification about birth from a doctor and/or midwife, or registration of an immigrant who are granted residence in Norway. In the case of birth registration, it is not mandatory with an ID control of the parents, and the mother herself is allowed to report home-birth [86]. In case of immigration, EEA citizens have their ID controlled by the Tax Administration while other foreign citizens have their ID controlled by the Norwegian Directorate of Immigration.

Valid EoI in the process of driving license issuance can be passport, previous driving license, bank card, military ID card, seaman's passport, postal ID card, travel certificate for refugees, immigrant's passport, foreign national's passports and ID cards from EEA countries [87]. In order to have a bank card issued, EoI can be passport, travel certificate for refugees, immigrant's passport, another bank card, driving license, military ID card, postal ID card, and ID cards from EEA countries [88].

To have a copy of a birth certificate issued, the only mandatory EoI is to provide the legitimate holder's name and national ID number. However, the birth certificate will only be sent to the legitimate holder's mail address registered in the National Registry.

## **6.0 Security gaps detected through fraud- and security analysis**

The security gaps listed below are revealed based on literature review and real-life fraud attack tests described previously in this work. While point 1, 5, 8, 9 and 10 are based on literature analysis, point 2, 3, 4, 6 and 7 originates from the fraud attack tests performed by the author.

### **6.1 Security gaps regarding ID proofing and verification**

1. European cooperation allows use of EoI from other EU countries. Such EoI are difficult for Norway to know the true evidence level of as Norway do not control their issuing routines. Indications that Norwegian ID proofing routines for EEA citizens are weaker than for other immigrants, increase the risk connected to EEA immigrants.
2. Documents like birth certificate, marriage certificate and similar are easy to falsify or fraudulently order, and therefore less trustable when used in ID proofing and verification.

3. The Norwegian national ID number can easily be guessed for anyone by anyone and therefore provide little EoI in ID proofing or verification.
4. ID proofing before allowing mail address change at the Tax Administration is weak. At the same time, many important services use mail address as one of the elements in processes very similar to ID proofing or verification, for example when issuing a birth certificate or bank card.
5. In Norway, ID proofing and verification processes often do not involve electronic biometric control with a cross check between IDs. The lack of such control makes imposter type ID fraud hard to detect.
6. A lack of notification to owner by mobile phone and/or email when important ID related events are performed (for example ordering new ID document or address change), makes successful ID fraud more difficult to detect than it have to be.
7. It is found indications that ID verification before ordering MinID access or changing BankID password is weak. For example a new BankID password can be received by mail after using only name and national ID number as authentication.
8. The National Registry is used as root EoI in Norway, but at the same time it does not include biometric information, meaning it lacks a direct link between the actual person and the ID registered, making ID proofing and verification unnecessary complicated.
9. The birth registration routine does not include mandatory ID control of the mother, which means children of unidentified parents cannot be securely ID proofed at a later stage.
10. Lack of possibilities to cross-check ID information in corroborative reference systems during ID proofing open possibilities that technical errors or attacks in one digital system alone can lead to wrong conclusions in ID proofing and verification processes.

## **6.2 Analysis on how current frameworks mitigate gaps**

There have been many frameworks developed for ID proofing and verification processes. Already mentioned are several national and international standards and guides [2,6,7,8,9,10, 11]. However, key objectives in ID proofing deviate between these sources. Taking ISO/ IEC 29003 [2] as a starting point, key objectives can be listed as follows:

- A:** To determine the ID is unique (duplication control)
- B:** To determine the ID exist (control against evidence that ID is not fictitious)
- C:** To determine the subject has some binding to the ID
- D:** To determine the ID is alive and in use (not belonging to a deceased)

In addition, two objectives not mentioned in ISO/IEC 29003, but mentioned by the UK's cabinet Office [8] and the Australian Attorney-General's Department [9] (**E**), and the Canadian Treasure Board Secretariat [7] (**F**) can be added:

- E:** To determine the ID is not used fraudulent (for example a blacklist control)
- F:** To determine the accuracy of the ID information

Point **A** deals with preventing attempts on registering an additional ID, duplicating either biometric information, biographical information or both. Electronic comparable biometric information is not stored in Norwegian registries today. Biographical information can however be controlled against duplication in Norwegian registries.

Point **B** deals with checking that the ID is present in registries. In Norway, the root EoI found in the National Registry is commonly used to control that a claimed ID exist.

Point **C** deals with a binding between the subject and the ID. This can be done by controlling biometrics between the ID document and the holder, for example through manual inspection of a portrait on an ID document.

Point **D** deals with checking that the ID has not a death reported on it, and that the ID is being used, for example paying taxes and being active on social media.

Point **E** deals with fraud control, for example checking fraud databases to control the ID has not been reported for fraudulent activity. It could for example be the actual document that is reported for fraud, or the biographic information, the type of ID document, or that the citizenship of origin is a high-risk country for a certain type of ID fraud. Such fraud databases could be everything from a local or national database like a library or driving license blacklist, to larger international ID document fraud databases like iFADO or DISCS.

Point **F** deals with the accuracy of the ID information. It could be some deviations in spelling of the name between ID documents, or it could be deviations between ID documents and the life story details given orally by the subject.

Table 6.1 summarizes how key objectives relates to the different security gaps identified. It can be seen that there is quite some overlap between how the different objectives cover different gaps.

**Table 6.1:** *Key objectives in ID proofing and verification and the gaps they can be assumed to reduce or eliminate.*

Key objectives in ID proofing and verification	Relevant gaps
<b>A:</b> To determine the ID is unique	1, 2, 5, 8, 9
<b>B:</b> To determine the ID exist	1, 2, 9, 10
<b>C:</b> To determine the subject has some binding to the ID	1, 2, 3, 4, 5, 7, 8, 9, 10
<b>D:</b> To determine the ID is alive and in use	1, 2, 9
<b>E:</b> To determine the ID is not used fraudulent	1, 2, 3, 4, 5, 6, 7, 8, 9, 10
<b>F:</b> To determine the accuracy of the ID information	1, 2, 5, 8, 9

Table 6.2 show the same objectives mapped to the previously mentioned standards and guides. Some objectives are mentioned in most standards and guides indicating they are more important. Also, one guide and one standard cover fewer objectives than the others - The Norwegian and the Canadian. The question whether it means these are weaker can be raised. However, some discretion has been used by the author in the work of checking boxes, meaning the reliability of the results of mapping guides and standards to key objectives can be discussed.

**Table 6.2:** How key objectives in ID proofing and verification are covered in a selection of guides and standards. The key objectives are derived from all the selected standards and guides (X = guide or standard cover the objective. / = guide or standard partly cover the objective).

Selected sources of key objectives in ID evaluation	Key objectives proposed by sources					
	A	B	C	D	E	F
<b>International Organization for Standardization</b> ISO/IEC 29003 – Identity proofing [2]	X	X	X	X		
<b>International Civil Aviation organization</b> Towards better practice in national ID management [11]	/	X	X	X		
<b>New Zealand Department of Internal Affairs</b> Evidence of identity standard [6]	/	X	X	X		
<b>Canadian Treasure Board Secretariat</b> Standard on Identity and Credential Assurance [7]	X		X			X
<b>UK's Cabinet Office</b> Identity proofing and verification of an individual [8]	X	X		X	X	
<b>Australian Attorney-General's Department</b> National Identity Proofing Guidelines [9]	X	X	X	X	X	
<b>Norwegian ID Network (draft stage)</b> Guide for ID establishment of physical persons [10]	X	X	X			

In this project, two weaknesses have been found in the ISO/IEC 29003 standard [2] when it comes to ID proofing and verification: I) It assume that a false or tampered ID document can be detected. That is not always the case, for example many countries do not have registers of all formats of old birth certificates. II) It does not make a separation between Physical Personal ID documents and Digital Personal ID documents, even though requirements to such ID documents can be quite different.

## 7.0 Proposing an Eol evaluation system to improve ID proofing and verification

Table 6.2 indicate that objective A, B, C and D could be regarded the most important as these are mentioned most. In addition, the UK framework [8] and the Australian guidelines [9] includes a control of ID against fraudulent use (objective E). This could be done fast if there is digital access to a blacklist or similar, and should therefore also be considered. When it comes to the Canadian guide's [7] objective to determine accuracy of ID information, this

refers to either ID control against an authoritative source or ID inspection by a trained examiner. It can be argued that control against authoritative sources already will be covered by previous listed objectives. Further, manual inspection by a trained examiner can be seen as too time consuming for a universal methodology, where any front desk officer should be able to perform the ID control. A short inspection should be performed, but it is unlikely that a thorough inspection will be performed by a front desk officer. This indicated that objective F can be ignored for simplicity reasons. Results from Table 6.1 also supports such a choice, as all security gaps affected by objective F are also affected by at least 3 other objectives as well. Based on this, the following work will mainly put weight on key objective A – E from subchapter 6.2.

For simplicity reasons, this report recommends understanding authoritative EoI like for example the centralized National Registry, or decentralized library registries, as digital ID documents. The author proposes to divide all ID documents in 3 sub-categories: I) **Digital Reference type ID documents (DRID)**, typically the National Registry, Driving License Registry and Passport Registry. II) **Digital Personal type ID documents (DPID)**, typically digital student ID, web-based Bank ID and similar, but also e-mail or facebook accounts and so on. III) **Physical Personal type ID documents (PPID)**, mainly classic ID documents like passport, driving license, bank card, birth certificate and so on.

### **7.1 Finding EoI values and using them for EoI evaluation**

EoI values of 1, 2 and 3 for ID documents (DRID, DPID and PPID), and 1, 2, 3, 4 and 5 for binding to subject, were chosen in this project for simplicity reasons. According to ISO/IEC 29003 [2] strength of EoI will come from three aspects:

- |   |  |
|---|--|
| <b>A)</b> The original identity proofing undertaken | <b>C)</b> The quality and robustness of the security features to prevent tampering, counterfeiting and forgery |
| <b>B)</b> The process used to issue it              |  |

In addition to these, the author proposes to add following three aspects:

- |  |  |
|--|--|
| <b>D)</b> Accountability/risk of prosecution | <b>F)</b> Available information to bind subject to ID document |
| <b>E)</b> Organizational measures            |  |



Use of EoI where fraud would result in prosecution (**D**) due to traceability would increase EoI strength. Traceability is a key aspect in information security. In addition, organizational security measures (**E**) are gaining more focus in information security, often connected to the ISO/IEC 27001 information security management system standard [89]. Last, it will be a need of available information to bind a subject to the ID document (**F**).

All these aspects are very transferrable to both DRID, DPID and PPID. From now on, when only the term “ID document” is used, it means all ID document types (both DRID, DPID and PPID).

## 7.2 EoI value requirements for ID documents

Table 7.1 show how this report proposes to map ID documents to EoI values. Acknowledging the value of a linkage between an ID document and a reference system, EoI value for DRID is added to EoI value of PPID or PDID as shown in subchapter 7.4.

**Table 7.1:** Requirements for ID documents. Letters at the left represents which of the EoI strength aspects above (chapter 7.1) the requirement mainly relates to.

Requirements which if all fulfilled gives EoI value 1	
1.(A)	It must not be possible to be enrolled in DRID or having issued PPID or PDID without any form of authentication (document accessibility)
2.(C)	The ID authority (for DRID, DPID, or PPID) must have some kind of mechanism to prevent unauthorized change of ID information (integrity)
3.(D)	It must be possible to hold one organization liable for ID document security breaches (traceability)
4.(F)	The ID document must present a unique ID in the application context, such as name, email address, social security number, etc.
Requirements which if all fulfilled gives EoI value 2	
1.	Point 2 - 3 in requirements EoI value 1 must be fulfilled
2.(A)	It must not be possible to be enrolled in DRID or having issued PPID or PDID without strong authentication (document accessibility)
3.(B)	An issuing party of DPID and PPID shall have a delivery process securing that ID documents will be delivered only to the correct person
4.(C)	Any ID document must include security elements providing moderate to high protection against fraud
5.(D)	Any ID registration shall be traceable to one employee at the EoI issuer
6.(D)	The rights to production and personalizing of any ID document shall be protected and reserved one special organization
7.(E)	An ID document issuing party shall have available routines concerning the application process and the production/personalization of the ID document
8.(E)	An issuing party of DPID and PPID shall have documented routines and processes for registering and reporting lost and stolen ID documents (fraud control)
9.(F)	The ID document must as a minimum contain: <ul style="list-style-type: none"> <li>-Holders full name and date of birth</li> <li>-A unique reference number or ID number</li> <li>-Face portrait or other biometrics with equivalent or better accuracy</li> </ul>

Requirements which if all fulfilled gives EoI value 3	
1.	Point 1 - 9 in requirements EoI value 2 must be fulfilled
2.(A)	There must be a control against duplicate identities as part of any ID establishment process, concerning; A) Information already exists, and B) Biometrics already exist
3.(E)	The responsible party shall have routines for periodically audits of all ID's registered
4.(E)	The responsible party shall have documented routines concerning the whole life cycle of the ID document in line with ICAO's best practice or at similar level

### 7.3 EoI value requirements for binding to subject

A strong link between an ID document and the subject can augment an EoI value derived unilateral from the ID document part. Requirements for EoI values associated with a single binding to subject, is suggested in this paper as illustrated in table 7.2.

**Table 7.2: Requirements for binding to subject**

	Manual Biometric match	Electronic Biometric match	Password or token corresponds	Interview corresponds	Written declaration corresponds
DPID EoI 1	EoI value 1	EoI value 1	EoI value 1	N/A	N/A
PPID EoI 1	EoI value 1	EoI value 1	EoI value 1	N/A	N/A
DRID EoI 1	EoI value 2	EoI value 2	EoI value 1	N/A	N/A
DPID EoI 2	EoI value 2	EoI value 2	EoI value 1	N/A	N/A
PPID EoI 2	EoI value 2	EoI value 2	EoI value 1	N/A	N/A
DRID EoI 2	EoI value 3	EoI value 3	EoI value 1	N/A	N/A
DPID EoI 3	EoI value 3	EoI value 4	EoI value 1	N/A	N/A
PPID EoI 3	EoI value 3	EoI value 4	EoI value 1	N/A	N/A
DRID EoI 3	EoI value 4	EoI value 5	EoI value 1	N/A	N/A
ID in general	N/A	N/A	N/A	EoI value 2	EoI value 3

As can be seen in table 7.2, there are possibilities to achieve an EoI value even without any ID document. Either through an interview, or through a reference person. Electronic biometric matches with physical ID documents must for security reasons only be based on an onboard chip or similar protected infrastructure. A biometric match for the same ID document should only be counted one time. For example, the EoI value from a manual biometric match should not be added to the EoI value from an electronic biometric match for the same ID document. The reason is that it will not give extra EoI when the binding is already confirmed at a higher level.

Passwords or tokens have been given the same EoI value independent of what EoI level it relates to since it can be assumed a security breach of a password or token would be equally likely to occur independent of what ID document it relates to.

#### **7.4 Calculating EoI level value based on multiple evidence and multiple bindings to subject – a methodological approach**

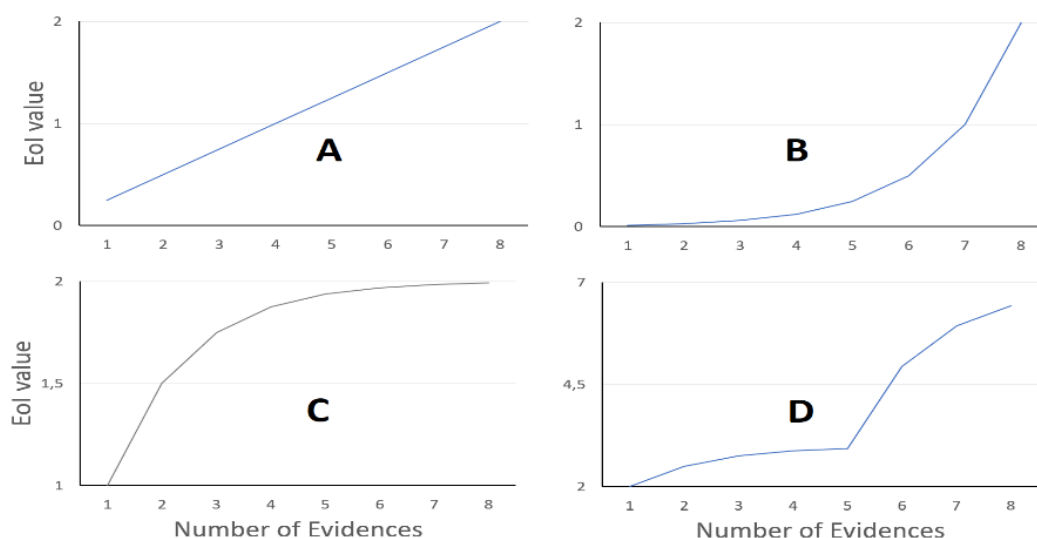
Combinations of ID documents in the proposed scheme will only add 50% of the value of the next additional document, resulting in a negative exponential function. This avoids that two ID documents with the same EoI value are considered twice as secure as one ID document, as would be the case by using a linear function (exemplified in Figure 7.1 A). Further, the negative exponential function will acknowledge the value of the first document unlike use of a positive exponential function (exemplified in Figure 7.1 B). The negative exponential function will also avoid that many ID documents with low EoI value can be combined to reach a high final EoI value (exemplified in Figure 7.1 C and D). The first part of the calculation algorithm proposed in this work:

$$P = D_1 + 2 \sum_{i=2}^N \frac{D_i}{2^i} \quad (3)$$

Where P is the *EoI Part value* resulting from this calculation, and D is the individual *ID Document's EoI value*. Note that Equation (3) is a convergent series so that the value P can be bound to a value which can be used to thwart the attempt to combine multiple low EoI value evidences to reach a high EoI value. In order to acknowledge the values of ID documents with high EoI values, these should be placed first in the algorithm. For example, D<sub>1</sub>: Passport, D<sub>2</sub>: Driving License, D<sub>3</sub>: Birth certificate. Now, EoI values for the binding to subject should be calculated and added separately to P, in a final EoI value calculation:

$$V = P + (B_1 + 2 \sum_{i=2}^N \frac{B_i}{2^i}) \quad (4)$$

Where B is EoI values of **B**indings to subject, and V is the *EoI level Value* used to map the combined EoI to the EoI level it corresponds to.



**Figure 7.1:** Characteristics of possible EoI value calculation methodologies: A: Characteristics of a linear function, B: Characteristics of a positive exponential function, C: Example of negative exponential function as proposed in this paper (using multiple ID documents at EoI value 1), and D: Example of negative exponential function as proposed in this paper (using one ID document with EoI value 2, four ID documents with EoI value 1, and three bindings to subject with EoI value 2).

Figure 7.1 C show that even multiple ID documents at EoI value 1 will not allow the achievement of EoI value 2. This is an advantage as these documents are so easy to forge. However, by adding any document with higher EoI value or a binding to subject, it will depending on its value allow to climb several EoI values (Figure 7.1 D). This system successfully stops attempts on use of multiple low-value ID documents or bindings to climb in the EoI hierarchy. The main advantage with the algorithm is that it gives such clear thresholds for what a subject can achieve with combined EoI of different values.

### 7.5 Mapping EoI level value to corresponding EoI levels

Calculation of an EoI level value could for example look like this: EoI level Value = Passport + (Manual biometric match of subject to PPID with EoI value 2 + Interview) equals  $V = D_1 + (B_1 + 2 * (\frac{B_2}{2^2}))$  equals  $V = 3 + (2 + 2 * (\frac{2}{4}))$  equals EoI level Value = 6. ISO/IEC 29003 [2] suggest use of 3 EoI levels (levels of identity proofing): low, moderate and high. However, in the ISO standard, the levels are based on qualitative evaluations. Three levels can also be used to map EoI level values found by quantitative techniques in this report to EoI levels as seen below. The thresholds are chosen based on the functions and the content of the proposed algorithm. The design assures that multiple ID documents with EoI value 1 cannot be used to

gain access to services at EoI level moderate. It also assures that EoI level high in practice is unreachable without both an ID document and a binding to subject where both offer a high EoI value.

**EoI level low** (EoI level value  $< 2$ )

$<$  equals less than

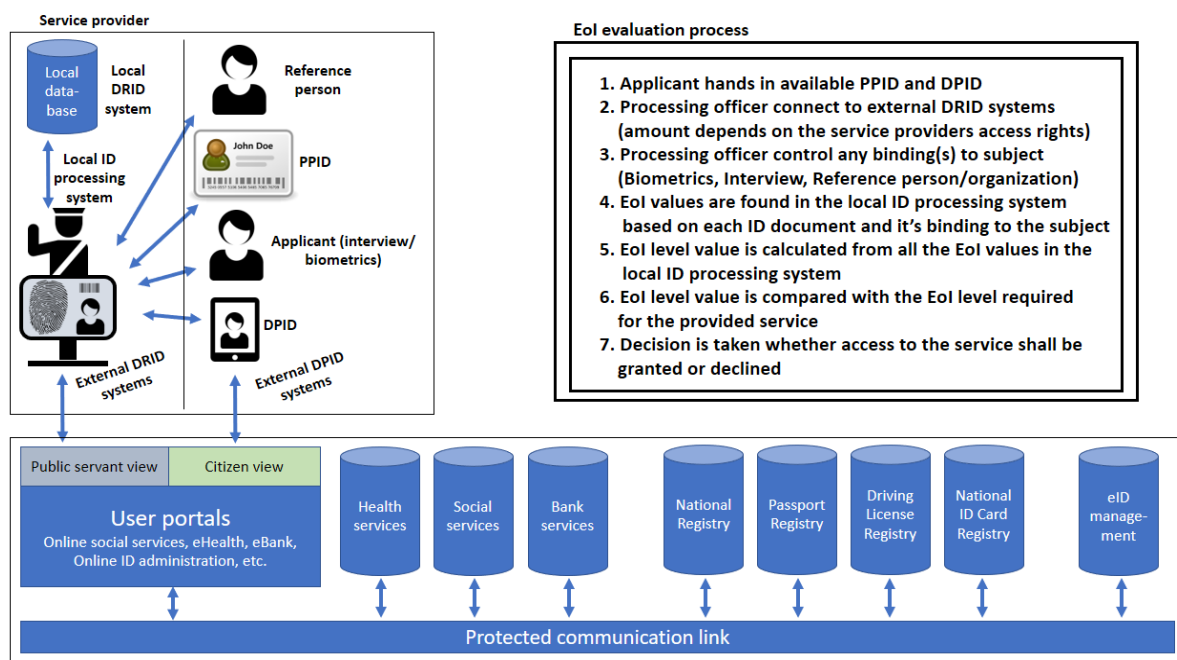
**EoI level moderate** (EoI level value  $\geq 2$  and  $< 6$ )

$\geq$  equals larger or equal to

**EoI level high** (EoI level value  $\geq 6$ )

## 7.6 The full EoI evaluation system

The infrastructure of the EoI evaluation system proposed in this paper is illustrated in figure 7.2. It shows core elements in the EoI evaluation process. The officer at the counter must decide if the necessary EoI level have been reached for the service applied for (for example to have a bank card issued). This evaluation process can be done with a high degree of automation through the unique EoI evaluation system proposed in this paper. The proposed EoI evaluation system will cover all ID proofing steps as described in ISO/IEC 29003 [2]; I) collect the proofing information, II) determine the veracity of the evidence collected against objectives, III) determine that identifying attributes from the EOI meet the required EoI level, and IV) bind the subject to the claimed identifying attributes.



**Figure 7.2:** Illustration of the EoI evaluation infrastructure of the proposed EoI evaluation system.

## 8.0 EoI systems that might come in the future

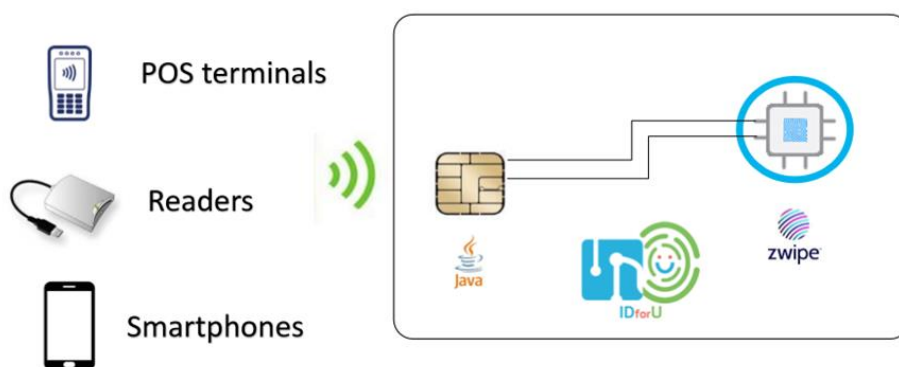
There are types of EoI systems that have the potential to change how ID documents are managed in near future. When discussing good practice for EoI evaluation it could be considered an advantage to know about such systems.

### *Biometrics based system without physical documents*

Australia has announced they want to use biometric scanning on airports instead of physical passports. It will be self-processing systems where travellers scan both face, iris and fingerprints. By 2020 the Australian government plans to process 90% of the travellers with no human contact [90]. This concept is also possible to apply for digital ID documents, where biometrics can be used as a token to access centrally stored biographic information.

### *Biometrics based system without need for central biometric registry access*

Combining biometrics and smart devices like phone, smartwatch, tablet, smartcard, etc. gives opportunities to authenticate people with the security of biometrics without the need of remote access to a biometric database. Instead, the person can be authenticated against the device, and the device can be authenticated against the system reading the device. Such a solution is illustrated by the IDforU project [91] in Figure 8.1. A smart card could be activated only when the holders finger is held over a fingerprint sensor. The smart card then authenticates the person based on biometrics, and then the card can be authenticated by another device communicating with a central system. It could be for example a hand-held terminal, a card reader or a smartphone. Since the device only have to authenticate the card and not the biometrics, this solution would be particularly privacy preserving.



**Figure 8.1:** IDforU project concept with Zwipe fingerprint card [91].

### ***Distributed system based on blockchain technology***

Blockchain technology works in the way that a network of computers is working together in storing events in a secure manner. By collecting events in blocks and distributing the blocks in a network of computers, secure hashed blocks of events can be stored incrementally without the risk of tampering. Since a network of nodes contains the blocks at any time, the content can be validated at any time by the network.

The way blockchain technology works, it will be possible to register links among ID attributes from different sources over time. Such sources might be passports, driving licenses, ID cards, social media accounts, email accounts, national eIDs, and so on. By chaining the history of ID attributes, it will be possible for parties with a need of ID proof to verify ID history and ID related links stored in the blockchains. This can be done in a privacy enhanced way by the use of encryption before registering on the blockchain and by the use of a private key to reveal the history or links. As an example the private key can be stored in a smartcard for universal use [92]. Such technology could also eliminate the need for physical documents like passports, ID cards and birth certificates, as data could be accessed by, and presented through, mobile devices like smart phones and tablets [93].

## **9.0 Discussion**

This Section has the purpose to state the authors interpretations and opinions of the fraud analysis and the proposed EoI evaluation system, and describe the work in light of previous literature on the field. It is also meant to explain the way this work has contributed to EoI evaluation techniques and give an understanding of the results in light of the research question. Last, it should give an understanding of how the proposed EoI evaluation system meets the need of its targeted users.

### ***9.1 Fraud analysis***

This work has identified gaps between secure ID proofing and verification systems and the way EoI is evaluated in Norway today. Examples found relates to many phases of the EoI lifecycle, spanning from birth registration to having a passport issued, and from address registration to obtaining access to a bank account. Even though physical security features of bank cards, driving licenses and passports are well developed, attacks following for example

imposter methodology or corruption are hard to detect. In addition, OSCE has described the variety and number of security features on current travel documents as a “double edged sword” for border control due to time limitations in checking security features at the border [40]. In cases like this, checking of corroborative evidence in a multi-modal ID proofing or verification system as proposed in this report could be of some help.

When it comes to ID document’s physical security features, it cannot be expected that all front desk officers shall know all the features of all possible ID documents. In addition, electronic systems for checking such features, not to mention biometrics, can still be considered too expensive for all types of organizations performing ID control. Therefore, demanding a certain combination of EoI depending on the risk associated with the service the subject want access to, might be a key to find the right level of assurance that the person in front of the officer is indeed the one he or she claim to be.

The main objective of ID related fraud is often connected to economic gain. One example is illegal labour, which could include several different scenarios. Examples could be I) false, stolen or borrowed ID documents used for border crossing to be able to live and work illegally in a country, II) false, stolen or borrowed ID documents used to establish an ID in a country for a non-citizen to be able to receive payment through legal channels, III) false, stolen or borrowed ID documents used to establish one or more additional IDs for reduced tax, responsibility-, or corporate related economic fraud, or IV) several workers are able to stay in a country for work reasons by using the same identity.

The situation in Norway where EEA citizens have their EoI controlled by the Tax Administration while other foreign citizens have their EoI more thoroughly controlled by the Norwegian Directorate of Immigration, is caused by the open border agreement within the Schengen area. Citizens in Schengen countries are allowed to travel freely across borders of Schengen countries and ID proofing is not an issue before the Schengen citizen decides to become a resident in Norway and/or applying for a work permit. It might be a need to increase background check of EEA citizens. To do so, it will probably be a need for a custom-made methodology which does not violate EEA agreements. Using EoI scores and levels in such a custom solution could be one way to solve this challenge.



It is not mandatory with an ID control of the parents before a birth registration. This can be seen as a risk as children in such cases will not be assigned a verifiable ID. It can also be raised a question if a lack of determining a secure ID of the child, either by not identifying the mother or by not collecting DNA or other biometrics from the child, could be considered a violation of the UN Convention on the Rights of the Child article 7 and 8 [94], stating any state's duty to preserve any child's ID. Using activity history from both child and parents could although help in evaluating the ID of these children as they grow up.

The most important ID document in Norway today, can be argued to be the individual electronic file in the Norwegian National Registry [82]. If the electronic file corresponds to the applicant, it will to a high degree confirm the identity exists and belongs to a living person. The National Registry is used as reference during issuance of Norwegian ID documents as illustrated in Table 9.1.

**Table 9.1:** ID documents where the Norwegian National Registry is used as source in the issuance process.

-Birth certificate	-Driving license	-Regular Passport
-Baptism certificate	-Citizen letter and citizen resolution	-Immigrants passport and travel certificate for refugees

[82,95] The list of ID documents is not complete.

The National Registry does not contain high level biometrics such as fingerprint or face portrait. Such a lack of a secure direct link between the ID and the person claiming the ID, might mean that ID fraud becomes easier than it has to be. This show the need of including corroborative evidence as proposed in this report, especially EoI including biometrics.

Results in this project further indicates that it is not as easy as one would believe it would be to get hold of falsified ID documents through the dark web. With prices for highly trusted ID documents ranging from around \$ 400 – 5000 [59], an investment like this would be far too risky as long as the seller are not giving any security that the buyer will receive any product. Probably even a desperate person would in most cases avoid taking such risk. This gives the impression this online activity is not real, and at least not happening in a huge scale as the

news media seem to claim. On the other hand, if someone have managed over time to build a trust relationship with someone on the dark web, it is easy to assume, like in the real world, it would be possible to purchase illegal ID documents also there. However, the dark web as a main market place for such business seem to be unrealistic based on online reviews and real-life testing performed in this project.

## **9.2 EoI evaluation**

Evidence fulfilling requirements of EoI value 1 would typically be a birth certificate, content of a facebook account, or a database registration at a library. Such evidence has low value as EoI since they are easy to falsify and difficult to validate. Evidence fulfilling requirements of EoI value 2 would typically be a bank card with portrait or a registration in the Driving License Registry. Such evidence provides more value as EoI since they contain more security features and has more secure issuance or registration processes. As an example, the physical driving license (EU type) have security features like holographic print, relief-pattern, UV print and IR features [76] and it can only be issued by physical appearance. This is in contrast to the Norwegian birth certificate which usually only contain security features like signature and stamp of document issuer, and can be delivered through mail after using the national ID number as authentication. Evidence fulfilling requirements of EoI value 3 would typically be a passport, or a registration in the Immigrant Registry. Such evidence is characterised by security features and issuing practices at a national level, since security breaches could cause severe consequences.

This report presents 3 EoI levels in chapter 7.5. Different standards and guidelines has made use of both 2, 3, 4 and 5 assurance levels. However, there are two good reasons for choosing 3 levels: I) ISO/IEC use 3 levels of identity proofing in their 29003 standard (although it also include a fourth zero-level) [2], and II) both the regulation eIDAS [43] as well as the proposed Cyber Security Act [44] make use of 3 assurance levels. Being in compliance with the most used standards on the field is important, but perhaps it is even more important to harmonise with legal regulations.

Mason [34] claimed that by using paper documents, a fabricated identity can be created overnight. However, attempting to create a false identity with an electronic biographical trail, according the author, will take far longer. The EoI evaluation system in this work does not

value a history trail in for example an email account as much as some form of authentication performed in the issuance process. It can be argued that a history trail going far back in time could be just as valuable as a superficial ID control before for example a digital student ID is issued. This might be a weakness in this work.

The EoI evaluation system proposed in this paper can be used in processes of deciding whether EoI provided by an applicant is at corresponding level with security requirements of the service provided by the organization. Characteristics of the EoI evaluation algorithm proposed in this paper are in line with recommendations for use of multiple EoIs [28,34,36, 37]. In addition, human factors such as uncertainty regarding choice of EoI level might be less present in a quantitative system compared to one based on qualitative evaluation. By pre-defining EoI belonging to each EoI value, organizations will no longer have a challenge in choosing which EoI to ask for in order to give access to their service. Such pre-definition should preferable be performed at a national level, and harmonized across Europe, assuring equality in EoI requirements between similar services.

A written declaration is given a quite high EoI value in this work, since EoI requirements in such cases to a certain degree can be transferred to the liable reference person. Further, manual biometric matches have been given significantly lower EoI values than electronic matches. This is based on research on manual and electronic face recognition. In 2014, White et al [96] found an average error rate of 10 % for 30 passport officers performing person to photo tests. 6 % of valid photos were wrongly rejected and 14 % of fraudulent photos were wrongly accepted. For photo to photo tests, results varied between 70.9 and 89.4 % correct. Frontex require face recognition systems at automatic border control stations to ensure a security level in terms of a false accept rate of 0,001 or less at a false reject rate not higher than 0,05 [97]. In a research project from 2015 performed by Opitz & Kriechbaum-Zabini [98] such error rates were achieved for 2 out of 3 biometric systems installed at Vienna international airport. It was also found that error rates varied based on remaining validity time of the passport (how old the portrait were) and country of passport (varying image quality between passport authorities). Face recognition technology is usually not fully automatic. Often identification accuracy can be quite poor, for example due to poor image quality. To solve this, face recognition applications often present a candidate list which for the operator to manually go through. The candidate list would consist of the highest matching images returned from the database [99]. It should probably, for the system proposed in this report, be

set a security level for use of electronic biometric matching somehow similar to the Frontex requirement.

It can happen that an applicant is not able in any way to achieve the EoI value corresponding to the required EoI level for a specific service. At the same time, the applicant can still have a legal right of access to that service. A possible solution for such cases could be to tag the applicant in the ID document, with the EoI value, or level, actually provided. This way the person can be followed up closer in the future, making sure the person is the single user of the ID, and does not use more than this one single ID. Such a methodology is already included in the new Norwegian National Registry Act which entered into force October 2017. The law requires IDs to be registered as “unique”, “controlled” or “not controlled” [100].

After finding several weaknesses in the Norwegian EoI system, the author discovered that many of the same weaknesses had already been pointed out before by both researchers and crooks. Still, the security holes had not been closed by the responsible parties. The proposed EoI evaluation system should, for the front desk officer’s convenience, be baked into a computer program with possibility to check off available EoI. This would ease the ID proofing and verification processes. Success of an EoI evaluation system like this depends on the organizations willingness to use it. History has shown that even when there are several tools available for controlling EoI, many of them have been utilized to a lesser extent, or not used at all. One example is passports which allows electronic biometric comparison. This possibility has to a small degree been taken advantage of in Norway, where manual control has been common [101]. If a solution is easy, fast, and at low cost, it is a greater chance it will be used.

ISO/IEC 29003 [2] focuses on ID uniqueness, existence and whether the applicant has a strong binding to the ID. The unique EoI evaluation system proposed in this report should provide trust in ID proofing and verification processes at level with main principles of ISO/IEC 29003 [2], as well as most other ID proofing work presented in this work. Table 6.1 in this report illustrate that all security gaps found in this work will be impacted positively as long as the proposed ID proofing and verification objectives are properly implemented. However, requirements in previous work are often given at a higher level, and leaves organizations to develop own methodology based on the recommendations. The work laid

down in this report show how these elements can be operationalized and fed into a quantitative system for easier and faster EoI evaluation.

The EoI evaluation system proposed in this report can be used in processes of deciding whether EoI provided by an applicant is at corresponding level with security requirements of the service provided by the organization. In 2008, Agbinya, Islam and Kwok [36] developed a digital identity management system using multi-modal authentication to address the issue of identity fraud and theft. They found that such a system would play a very big role in reducing cases of identity theft and fraud on online services. It can be argued the same effect should be found in a multi-modal EoI evaluation system as proposed in this report. Further basis for this assumption is the results from the Norwegian ID Centre showing that 659 people were caught performing 787 cases of ID document fraud in 2013, indicating it was common to carry only one fraudulent ID document for each person [47].

## **10.0 Conclusion and remarks**

Work laid down in this project show that there are gaps between secure ID proofing and verification systems and the way EoI is evaluated in Norway today. Many ID fraud scenarios are still possible in Norway, even though some of them were revealed several years ago. This work has also shown indications that some of the concerns regarding ID document sale on the dark web might happen at a smaller scale than anticipated.

The methodology for EoI evaluation proposed in this paper can be used to assign different EoIs appropriate EoI values. Further, by the use of an algorithm, their combined EoI value can be mapped to a functional EoI level. ISO/IEC 29003 [2] focuses on ID uniqueness, existence and whether the subject has a strong binding to the ID. The unique EoI evaluation system proposed in this report will have a positive impact on all the security gaps found in this project. It can also be argued it will provide trust in ID proofing and verification processes at level with main principles of the ISO standard, as well as most other ID guides and standards presented in this work. The work laid down in this report show how these principles can be operationalized and fed into a quantitative system for easier and faster EoI evaluation.

This report has proposed a ready-to-test EoI evaluation system. In the future, developing an application allowing real-life testing of the proposed EoI evaluation system, would be a

natural next step. It is hard to estimate the presumable effect of the proposed EoI evaluation system, since it has not been tested in practice. As testing of such a system would be time consuming and cooperation demanding from different stakeholders, this limited work has focused on developing a system model instead of testing its performance in operation. This leaves it to any interested party to test the system in practice over a time period in order to evaluate its true performance.

## 11.0 Reference list

1. Chamberlain, D. (2016). Identity Management Infrastructure: What is Evidence of Identity? [Online] URL: <https://www.icao.int/Meetings/icaotrip-Iran-2016/Documents/Presentations/3%20CHAMBERLAIN.pdf>
2. International Organization for Standardization (2016). ISO/IEC DIS 29003 Information technology – Security techniques – Identity proofing 2016-11-07
3. Dharwadker, S. (2017). Evidence of Identity – Taking-Off [Online]. URL: <https://www.icao.int/Meetings/TRIP-HongKong-2017/Documents/1%20DHARWADKER%20SANJAY.pdf>
4. Javelin (2017). Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study [Online]. URL: <https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new>
5. Experian, PKF Littlejohn & University of Portsmouth's Centre for Counter Fraud Studies (2016). Annual fraud indicator [Online]. URL: <http://www.port.ac.uk/media/contacts-and-departments/icjs/ccfs/Annual-Fraud-Indicator-2016.pdf>
6. New Zealand Department of Internal Affairs (2009). Evidence of Identity Standard [Online]. URL: <https://www.dia.govt.nz/Resource-material-Evidence-of-Identity-Standard-Index>
7. Canadian Treasury Board Secretariat (2013). Standard on Identity and Credential Assurance [Online]. URL: <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776>
8. UK's Cabinet Office (2014). Identity proofing and verification of individual [Online]. URL: <https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual>
9. Australian Attorney-General's Department (2016). National Identity Proofing guidelines [Online]. URL: <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/NationalIdentityProofingGuidelines.PDF>
10. Norwegian ID Network (2016). Veileder i fastsettelse av identitet til fysiske personer. Norway, Oslo (in press)
11. International Civil Aviation Organization (2013). Machine readable travel documents – to-wards better practice in national identification management [Online]. URL: <https://www.icao.int/Security/mrtd/Documents/TR%20-%20%20EOI%20Version%20Release%203%20Draft%2030%20April%202013.pdf>
12. ORIGINS (2015). Recommendations for Reliable Breeder Documents [Online]. URL: <http://www.origins-project.eu/>
13. Standard Norge (2017). Én grunnleggende identitet [Online]. URL: <https://www.standard.no/nyheter/nyhetsarkiv/ikt/2017/en-grunnleggende-identitet/>
14. De Rosa, I. (2015). UDI: Politiets ID-kontroll bør bli bedre [Online]. URL: [https://www.nrk.no/norge/udi\\_-\\_politiets-id-kontroll-bor-bli-bedre-1.12718659](https://www.nrk.no/norge/udi_-_politiets-id-kontroll-bor-bli-bedre-1.12718659)
15. Fladby, M. (2009). ID utfordringer for NAV [Online]. URL: <https://www.slideshare.net/Utlendingsdirektoratet/udis-vrkonferanse-2009-id-utfordringer-for-nav>
16. Remen, A. C. & Reinholdtsen, L. (2016). Skattedirektøren: ID-sjekk av utlendinger er for dårlig [Online]. URL: <https://www.nrk.no/norge/sjekker-ikke-id-godt-nok-1.12794326>

17. Rørslett, K. & Brekke, A. (2013). Klarer ikke å sjekke falsk ID [Online]. URL: <https://www.nrk.no/norge/klarere-ikke-a-sjekke-falsk-id-1.11370176>
18. Norwegian ID Centre (2014). Kartlegging av ID-arbeid [Online]. URL: <https://www.nidsenter.no/globalassets/vedlegg/nid-rapporter/evaluering---del-2.pdf>
19. Valgdirektoratet (2017). Stortings- og sametingsvalget 2017 [Online]. URL: <https://valg.no/globalassets/dokumenter/valgmateriell/informasjonsbrosjyrer/valgbrosjyre-bokmal.pdf>
20. Lien, Ø. F. (2017). - Uklare krav til id-kontroll [Online]. URL: <https://www.oa.no/valg2017/informasjossikkerhet/ntnu-i-gjovik/uklare-krav-til-id-kontroll/s/5-35-487432>
21. National ID Centre (2013). ID-nettverkets bakgrunn [Online]. URL: [https://www.nidsenter.no/fag/innholdsside\\_id-nettverket/innholdsside-om-opprettelsen/](https://www.nidsenter.no/fag/innholdsside_id-nettverket/innholdsside-om-opprettelsen/)
22. Leedy, P. & Ormrod, J. E. (2013). Practical Research – Planning and design. USA, Pearson
23. Yang, C. (2014). Fingerpring biometrics for ID document verification. Industrial electronics and applications: 1441-1445
24. Paunwala, M. C. & Patnaik, S. (2010). Sheltered Identification with Hiding Biometrics. Signal and Image Processin: 191-196
25. Fairhurst, M. C. (2003). Document identity, authentication and ownership: the future of biometric verification. IEEE Conference Publications: 1108-1116
26. Thein, H. H., Sein, M. M. & Aung, S. N. L. (2007). A reliable technique for personal identification or verification. IEEE Conference Publications: 265-269
27. Elliott, S.E., Massie, S. A. & Sutton, M. J. (2007). The Perception of Biometric Technology: A Survey. IEEE Conference Publications: 259-264
28. Yang, B., Busch, C., Bringer, J. et. al. (2013). Towards standardizing trusted evidence of identity. Proceedings of the 2013 ACM workshop on Digital identity management: 63-72
29. Ursin, L. H. (2007). ID-tyveri er for enkelt [Online]. URL: <https://forskning.no/internett-kriminalitet/2008/02/id-tyveri-er-enkelt>
30. Støbakk, T. (2016). Mann og kvinne skal ha robbet postkassene til over 1000 mennesker [Online]. URL: <https://www.dagbladet.no/nyheter/mann-og-kvinne-skal-ha-robbet-postkassene-til-over-1000-mennesker/63975206>
31. Finans Norge (2017). ID-tyveri kan være ødeleggende [Online]. URL: <https://www.finansnorge.no/aktuelt/nyheter/2017/10/id-tyveri-kan-vare-odeleggende/>
32. European Association for Biometrics (2016). Norsk biometri forum meeting [Online]. URL: <https://www.eab.org/events/program/133?ts=1509047010091>
33. International Civil Aviation Organization (2010). Guide for assessing security of handling and issuance of travel documents [Online]. URL: <https://www.iom.int/jahia/webdav/shared/shared/mainsite/activities/tcm/Assessment-Guide-PART1-Best-Practices-Jan-2010.pdf>
34. Mason, S. (2004). Validating identity for the electronic environment. IET Conference Publications: 54-70
35. Evans-Pughe, C. (2008). A crisis of identity. Engineering & Technology: 16-18
36. Agbinya, J. I., Islam, R. & Kwok, C. (2008). Development of digital environment identity (DEITY) system for online access. Third International Conference on Broadband Communications, Information Technology & Biomedical Applications: 1-8



37. Wu, L., Ping, R., Donghong, S. et. al. (2012). Research in techniques of personal identity management. IEEE Conference Publications: 912-915
38. FIDELITY (2012). About FIDELITY [Online]. URL: <http://www.fidelity-project.eu/>
39. European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (2011). Operational and technical security of electronic passports [Online]. URL: [http://frontex.europa.eu/assets/Publications/Research/Operational\\_and\\_Technical\\_Security\\_of\\_Electronic\\_Pasports.pdf](http://frontex.europa.eu/assets/Publications/Research/Operational_and_Technical_Security_of_Electronic_Pasports.pdf)
40. Organization for Security and Co-operation in Europe (2013). Addressing the link between travel document security and population registration/civil registration documents and processes [Online]. URL: <http://www.osce.org/secretariat/110610?download=true>
41. FIDO alliance (2017). FIDO UAF architectural overview [Online]. URL: <https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-uaf-overview-v1.1-id-20170202.pdf>
42. Buypass (2017). eIDAS – mer effektiv elektronisk samhandling i Europa [Online]. URL: <https://www.buypass.no/ressurser/eidas-europeisk-elektronisk-samhandling>
43. eIDAS (2014). Regulation on electronic identification and trust services for electronic transactions in the internal market [Online]. URL: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN>
44. Cybersecurity act (2017). Proposal for a regulation on information and communication technology cybersecurity certification [Online]. URL: [https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477\\_en](https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en)
45. Council of the European Union (2017). The Council of the EU PRADO Glossary, explaining technical terms related to security features, and to security documents in general [Online]. URL: [https://www.parlament.gv.at/PAKT/EU/XXV/EU/14/04/EU\\_140473/imfname\\_10713382](https://www.parlament.gv.at/PAKT/EU/XXV/EU/14/04/EU_140473/imfname_10713382)
46. Norwegian ID Centre (2015). Misbruk av ID-dokumenter 2014 [Online]. URL: [https://www.nidsenter.no/Global/Publikasjoner/NID\\_Brosjyre\\_2014\\_web\\_endelig.pdf](https://www.nidsenter.no/Global/Publikasjoner/NID_Brosjyre_2014_web_endelig.pdf)
47. Norwegian ID Centre (2014). Misbruk av ID-dokumenter 2013 [Online]. URL: [https://www.nidsenter.no/Global/Publikasjoner/misbruktedokumenter\\_2013.pdf](https://www.nidsenter.no/Global/Publikasjoner/misbruktedokumenter_2013.pdf)
48. Spiegel (2011). An Eye for an Eye: The Anatomy of Mossad's Dubai Operation [Online]. URL: <http://www.spiegel.de/international/world/an-eye-for-an-eye-the-anatomy-of-mossad-s-dubai-operation-a-739908.html>
49. Schult, C. & Stark, H. (2010). The Dubai Assassins: Alleged Killer Left Traces in Cologne and Israel [Online]. URL: <http://www.spiegel.de/international/world/the-dubai-assassins-alleged-killer-left-traces-in-cologne-and-israel-a-679530.html>
50. Landytown (without year) Beware of Michael the 'Deutschman' from NL [Online]. URL: [http://landytown.myfastforum.org/archive/beware-of-michael-the-deutschman-from-nl\\_o\\_t\\_t\\_9367.html](http://landytown.myfastforum.org/archive/beware-of-michael-the-deutschman-from-nl_o_t_t_9367.html)
51. ynetnews (2010) Report: German passport used by Dubai hit squad not forged [Online]. URL: <http://www.ynetnews.com/articles/0,7340,L-3851926,00.html>
52. Spiegel (2012). Cats and camper vans: The bizarrely normal life of the Neo-Nazi terror cell. URL: <http://www.spiegel.de/international/germany/cats-and-camper-vans-the-bizarrely-normal-life-of-the-neo-nazi-terror-cell-a-816966.html>

53. NSU LEAKS (2016). War Mundlos von 1998 bis 2011 "Max Florian Burkhardt"? URL: <http://arbeitskreis-n.su/blog/2015/11/26/war-mundlos-von-1998-bis-2011-max-florian-burkhardt/>
54. CBCnews (2009). Italian police arrest Mumbai attack suspects [Online]. URL: <http://www.cbc.ca/news/world/italian-police-arrest-mumbai-attack-suspects-1.790373>
55. Wikipedia (2016). Irish passport [Online]. URL: [https://en.wikipedia.org/wiki/Irish\\_passport#Notable\\_cases\\_of\\_purported\\_fraudulent\\_use](https://en.wikipedia.org/wiki/Irish_passport#Notable_cases_of_purported_fraudulent_use)
56. Oppegård, G. G. (2012). Nekter for at utlendinger urettmessig er blitt norske statsborgere [Online]. URL: <http://www.tv2.no/a/3871926/>
57. Verdens Gang (2012). 58.000 utlendinger registrert som norske statsborgere etter datatabbe [Online]. URL: <http://www.vg.no/nyheter/innenriks/58-000-utlendinger-registrert-som-norske-statsborgere-etter-datatabbe/a/10068558/>
58. Haakaas, E. (2012). 58.000 utlendinger ble norske etter datatabbe [Online]. URL: <https://www.aftenposten.no/norge/58000-utlendinger-ble-norske-etter-datatabbe-144878b.html>
59. Norsk rikskringkasting (2015). Passmannen [Online]. URL: <http://www.nrk.no/dokumentar/xl/passmannen-1.12404097>
60. Widerøe, R. J., Tommelstad, B., Andersen, G. & Hopperstad, M. S. (2016). Bløffmakerne [Online]. URL: <http://www.vg.no/spesial/2016/slik-jobbet-bloffmakerne/>
61. Holm, P. A. & Dragland, L. L. (2011). Fikk millionstøtte til barn som ikke eksisterte [Online]. URL: <http://www.aftenposten.no/nyheter/iriks/Fikk-millionstotte-til-barn-som-ikke-eksisterte-6667444.html>
62. Johansen, P. A. (2013). Har slettet 70 falske barn i Folkeregisteret [Online]. URL: <http://www.aftenposten.no/nyheter/iriks/Har-slettet-70-falske-barn-i-Folkeregisteret-7118493.html>
63. Dragland, L. L. & Haakaas, E. (2014). Snekker med syv falske navn svindlet Nav for over en halv million [Online]. URL: <https://www.aftenposten.no/norge/i/oRr0K/Snekker-med-syv-falske-navn-svindlet-Nav-for-over-en-halv-million>
64. SVT (2015). Lätt att få tag på falska id-handlingar [Online]. URL: <https://www.svt.se/nyheter/lokalt/vast/latt-att-fa-tag-pa-falska-id-handlingar>
65. SalePassportsFake.cc (2017). FakeID [Online]. URL: [http://www.salepassportsfake.cc/novelty\\_fake\\_id\\_pricing.shtml](http://www.salepassportsfake.cc/novelty_fake_id_pricing.shtml)
66. Complaints Board (2017) www.buyfakepassports.com [Online]. URL: <https://www.complaintsboard.com/complaints/wwwbuyfakepassportscom-c186116.html>
67. ComplaintWire (2014). Fake Passports [Online]. URL: <https://complaintwire.org/complaint/7dsUqiZOAwy/http-www-buyfakepassport-cc>
68. Skatteetaten (2017). Fødselsnummer [Online]. URL: <http://www.skatteetaten.no/no/Person/Folkeregister/Fodsel-og-navnevalg/Barn-fodt-i-Norge/Fodselsnummer/>
69. Wikipedia (2017). Fødselsnummer [Online]. URL: <https://no.wikipedia.org/wiki/F%C3%B8dselsnummer>
70. Difi (2017). Slik skaffer du deg elektronisk ID [Online]. URL: <http://eid.difi.no/nb/id-porten/slik-skaffer-du-deg-elektronisk-id>
71. Difi (2017). Glamt password [Online]. URL: <http://eid.difi.no/nb/bankid/glemt-passord>

72. Nordea (2017). Glemte passord eller brukernavn? [Online]. URL: <https://www.nordea.no/privat/daglig-bruk/internett-mobil-og-telefon/glemte-passord-eller-brukernavn.html>
73. International Civil Aviation Organization (2015). Doc Series – Doc 9303 [Online]. URL: <https://www.icao.int/publications/pages/publication.aspx?docnum=9303>
74. Lovdata (2017) Lov om pass (passloven) [Online]. URL: <https://lovdata.no/dokument/NL/lov/1997-06-19-82>
75. Belser, R. (2013). The weakest link in the Identity chain [Online]. URL: <https://www.icao.int/Meetings/mrtd-SintMaarten2013/Documents/12-Belser.pdf>
76. Statens Vegvesen (2013). Nytt norsk førerkort fra 19. januar 2013 [Online]. URL: [https://www.vegvesen.no/\\_attachment/493459/binary/801365?fast\\_title=Nytt+f%C3%B8rerkerkort+19.+januar+2013+-+brosjyre.pdf](https://www.vegvesen.no/_attachment/493459/binary/801365?fast_title=Nytt+f%C3%B8rerkerkort+19.+januar+2013+-+brosjyre.pdf)
77. Statens Vegvesen (2016). Førerkortets sikkerhetslementer [Online]. URL: <https://www.vegvesen.no/forerkort/har-forerkort/gyldig-forerkort-i-norge/eos-modell-2/sikkerhetslementer>
78. Statens Vegvesen (2016) Førerkortets sikkerhetslementer [Online]. URL: <https://www.vegvesen.no/forerkort/har-forerkort/gyldig-forerkort-i-norge/eos-modell-1/Sikkerhetslementer>
79. Statens Vegvesen (2014). Høringsnotat – hjemmel for behandling av personopplysninger på vegtrafikkområdet [Online]. URL: [https://www.vegvesen.no/\\_attachment/582651/binary/932623?fast\\_title=H%C3%B8ringsnotat.pdf](https://www.vegvesen.no/_attachment/582651/binary/932623?fast_title=H%C3%B8ringsnotat.pdf)
80. Bits (2017). Bankkort [Online]. URL: <http://www.bits.no/bank/bankkort/>
81. Lov om statsborgerskap (2005). LOV-2005-06-10-51 (Statsborgerloven) [Online]. URL: <https://lovdata.no/dokument/NL/lov/2005-06-10-51>
82. The Norwegian Tax Administration (2017). This is the National Registry [Online]. URL: <http://www.skatteetaten.no/en/person/National-Registry/This-is-the-National-Registry/>
83. Justis- og Politidepartementet (2007). Nasjonalt ID-kort [Online]. URL: <https://www.regjeringen.no/globalassets/upload/JD/Vedlegg/ID-kort-Sluttrapport.pdf>
84. digi.no (2016). Lover nasjonalt digitalt ID-kort etter årevis med utsettelse [Online]. URL: <https://www.digi.no/artikler/lover-nasjonalt-digitalt-id-kort-etter-arevis-med-utsettelse/347998>
85. The Norwegian National Police (2017). Søke om pass [Online]. URL: <https://www.politiet.no/en/services/pass/soke-om-pass/>
86. Lov om folkeregistrering (2017) LOV-2016-12-09-88 (Folkeregisterloven). URL: <https://lovdata.no/dokument/NL/lov/2016-12-09-88?q=folkeregister>
87. The Norwegian Public Roads Administration (2016). Gyldig legitimasjon [Online]. URL: <https://www.vegvesen.no/forerkort/ta-forerkort/gyldig-legitimasjon>
88. Finans Norge (2016). Hvorfor må banken kontrollere og bekrefte en persons identitet? [Online]. URL: [https://www.finansnorge.no/globalassets/kundekontroll/hvorfor-ma-banken-kontrollere-og-bekrefte-en-persons-id\\_des15.pdf](https://www.finansnorge.no/globalassets/kundekontroll/hvorfor-ma-banken-kontrollere-og-bekrefte-en-persons-id_des15.pdf)
89. International Organization for Standardization (2013). ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems - Requirements
90. Dutton, P. (2016). Benefits for consumers, travellers and industry from red tap cuts and new technology [Online]. URL:

- <http://www.minister.border.gov.au/peterdutton/2015/Pages/benefits-for-consumers-travellers-industry.aspx>
91. Guo, Q. (2016). Email correspondence regarding the IDforU research project
  92. Maxim, J. (2015). Onename Launches Blockchain Identity Product Passcard [Online]. URL: <https://bitcoinmagazine.com/articles/onename-launches-blockchain-identity-product-passcard-1431548450/>
  93. SITA (2016). SITA explores travel identity of the future [Online]. URL: <https://www.sita.aero/pressroom/news-releases/sita-explores-travel-identity-of-the-future>
  94. United Nations (1990). Convention on the Rights of the Child [Online]. URL: <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx>
  95. Den Norske Kirke (2012). Dåp – Dåp av små og store [Online]. URL: <http://www.eidsvoll.kirken.no/Forsiden/Aktuelt/ArticleId/3862/Dap-24>
  96. White, D., Kemp, R. I., Jenkins, R., Matheson, M. & Burton, A. M. (2014). Passport officers errors in face matching [Online]. URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4136722/pdf/pone.0103510.pdf>
  97. European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (2015). Best practice technical guidelines for automated border control (ABC) systems [Online]. URL: [http://frontex.europa.eu/assets/Publications/Research/Best\\_Practice\\_Technical\\_Guidelines\\_ABC.pdf](http://frontex.europa.eu/assets/Publications/Research/Best_Practice_Technical_Guidelines_ABC.pdf)
  98. Opitz, A. & Kriechbaum-Zabini, A. (2015). Evaluation of face recognition technologies for identity verification in an egate based on operational data of on airport. International conference on advanced video and signal based surveillance, p. 1-5
  99. White, D., Dunn, J. D., Schmid, A. C. & Kemp, R. I. (2015). Error rates in users of automatic face recognition software [Online]. URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4605725/pdf/pone.0139827.pdf>
  100. Stortinget (2016) Vedtak til lov om folkeregistrering (folkeregisterloven) [Online]. URL: <https://www.stortinget.no/no/Saker-og-publikasjoner/Vedtak/Beslutninger/Lovvedtak/2016-2017/vedtak-201617-009/>
  101. Nilsen, K. S., Solheim, S. & Stolt-Nielsen, H. (2016) Politiet: Automatisk passkontroll løser ikke utfordringene på Oslo lufthavn [Online]. URL: [https://www.nrk.no/norge/politiet\\_-automatisk-passkontroll-loser-ikke-problemene-1.13116489](https://www.nrk.no/norge/politiet_-automatisk-passkontroll-loser-ikke-problemene-1.13116489)

## 12.0 Appendix

### 12.1 Abbreviations

<b>DISCS</b>	Document Information System Civil Status
<b>DPID</b>	Digital Personal type ID document
<b>DRID</b>	Digital Reference type ID document
<b>eIDAS</b>	Regulation on electronic identification and trust services for electronic transactions in the internal market
<b>EoI</b>	Evidence of Identity
<b>FIDELITY</b>	Fast and trustworthy identity delivery and check with ePassports leveraging traveller privacy
<b>FIDO</b>	Fast Identity Online
<b>FRONTEX</b>	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
<b>ICAO</b>	The International Civil Aviation Organization
<b>ID</b>	Identity
<b>iFADO</b>	intranet False and Authentic Documents Online
<b>IR</b>	Infrared
<b>ISO</b>	The International Organization for Standardization
<b>ORIGINS</b>	Restoring e-passport confidence and leveraging extended border security
<b>OSCE</b>	Organization for Security and Co-operation in Europe
<b>PPID</b>	Physical Personal type ID document
<b>RFID</b>	Radio Frequency Identification
<b>TOR</b>	The Onion Router

### 12.2 List of figures

FIGURE 2.1: OVERVIEW OF THE IDENTITY PROOFING AND VERIFICATION PROCESS BY THE UK'S CABINET OFFICE [8]. .....	15
FIGURE 2.2: KEY PRINCIPLES THAT ARE CENTRAL TO MOST EOI FRAMEWORK STANDARDS [11]. .....	17
FIGURE 2.3: AUTHENTICATION MESSAGE FLOW [45]. .....	18
FIGURE 3.1: COMMON FRAUD METHODOLOGY FOR ID DOCUMENTS [48]. .....	20
FIGURE 3.2: DIFFERENT TYPES OF ID DOCUMENT FRAUD REVEALED IN NORWAY IN 2014 [49,50]. ACCORDING TO THE NORWEGIAN ID CENTRE THE CATEGORY "OTHER DOCUMENTS" INCLUDES DOCUMENTS LIKE MILITARY ID, MARRIAGE CERTIFICATE AND TRANSCRIPTS FROM THE NATIONAL REGISTRY. ....	21

FIGURE 3.3: ACCORDING TO LANDYTOWN AND YNET NEWS, THE FIGURE SHOWS THE PASSPORT OF “MICHAEL BODENHEIMER” [53], AND A LIST OF SUSPECTED HIT SQUAD MEMBERS [54].	22
FIGURE 3.4: ACCORDING TO NSU LEAKS, THE FIGURE SHOWS THE PASSPORT OF UWE MUNDLOS WITH MAX FLORIAN BURKHART’S IDENTITY [56].	23
FIGURE 4.1: WEBSITE OFFERING FALSIFIED ID DOCUMENTS ON THE WEB [68].	26
FIGURE 4.2: HALLWAY WHERE NEW MAIL BOX WAS INSTALLED. 1) BEFORE MAILBOX IS INSTALLED. 2) AFTER MAILBOX IS INSTALLED.	31
FIGURE 5.1: OVERVIEW OF COMMONLY USED NORWEGIAN ID DOCUMENTS. THE OVERVIEW WAS DEVELOPED AS PART OF THIS PROJECT. COLOURS ARE USED FOR VISUALIZATION ONLY AND HAVE NO FUNCTION. YEAR ILLUSTRATE WHEN A NEW VERSION CAME AND AN OLD VERSION WAS PHASED OUT.	35
FIGURE 5.2: AN EPASSPORT SPECIFIED BY ICAO’S DOCUMENT 9303 CONTAINS BOTH VISIBLE AND INVISIBLE SECURITY FEATURES. IT ALSO HAS AN EMBEDDED RFID CHIP, WHICH CONTAINS BIOMETRIC DATA LIKE FACE, FINGERPRINT AND IRIS IMAGES [78].	36
FIGURE 5.3: A DRIVING LICENSE WITH UV LIGHT IN THE UPPER RIGHT CORNER AND HOLOGRAMS IN THE LOWER LEFT CORNER [79].	37
FIGURE 5.4: A) NORWEGIAN BANK CARD WITH UV AND MICRO FEATURES. B) VISA CARD WITH DOVE HOLOGRAM AND SIGNATURE FIELD. C) MASTERCARD WITH WORLD MAP HOLOGRAM AND SIGNATURE FIELD [83].	38
FIGURE 5.5: A) NORWEGIAN BIRTH CERTIFICATE FROM AROUND 2014 (BLANK). B) NORWEGIAN BIRTH CERTIFICATE FROM 1982 (TEXT AND SIGNATURE REMOVED). BOTH ARE PRINTED ON REGULAR PAPER AND USE SIGNATURE AND STAMP AS ONLY SECURITY FEATURES.	39
FIGURE 5.6: WINNER OF DESIGN COMPETITION FOR NORWEGIAN ID CARD. FINAL DESIGN MIGHT HOWEVER DEVIATE FROM THE PICTURE [86].	40
FIGURE 7.1: CHARACTERISTICS OF POSSIBLE EOI VALUE CALCULATION METHODOLOGIES: A: CHARACTERISTICS OF A LINEAR FUNCTION, B: CHARACTERISTICS OF A POSITIVE EXPONENTIAL FUNCTION, C: EXAMPLE OF NEGATIVE EXPONENTIAL FUNCTION AS PROPOSED IN THIS PAPER (USING MULTIPLE ID DOCUMENTS AT EOI VALUE 1), AND D: EXAMPLE OF NEGATIVE EXPONENTIAL FUNCTION AS PROPOSED IN THIS PAPER (USING ONE ID DOCUMENT WITH EOI VALUE 2, FOUR ID DOCUMENTS WITH EOI VALUE 1, AND THREE BINDINGS TO SUBJECT WITH EOI VALUE 2).	50
FIGURE 7.2: ILLUSTRATION OF THE EOI EVALUATION INFRASTRUCTURE OF THE PROPOSED EOI EVALUATION SYSTEM.	51
FIGURE 8.1: IDFORU PROJECT CONCEPT WITH ZWIPE FINGERPRINT CARD [89].	52

### 12.3 List of tables

TABLE 6.1: KEY OBJECTIVES IN ID PROOFING AND VERIFICATION AND THE GAPS THEY CAN BE ASSUMED TO REDUCE OR ELIMINATE.	44
TABLE 6.2: HOW KEY OBJECTIVES IN ID PROOFING AND VERIFICATION ARE COVERED IN A SELECTION OF GUIDES AND STANDARDS. THE KEY OBJECTIVES ARE DERIVED FROM ALL THE SELECTED STANDARDS AND GUIDES (X = GUIDE OR STANDARD COVER THE OBJECTIVE. / = GUIDE OR STANDARD PARTLY COVER THE OBJECTIVE).	45
TABLE 7.1: REQUIREMENTS FOR ID DOCUMENTS. LETTERS AT THE LEFT REPRESENTS WHICH OF THE EOI STRENGTH ASPECTS ABOVE (CHAPTER 7.1) THE REQUIREMENT MAINLY RELATES TO.	47
TABLE 7.2: REQUIREMENTS FOR BINDING TO SUBJECT	48
TABLE 9.1: ID DOCUMENTS WHERE THE NORWEGIAN NATIONAL REGISTRY IS USED AS SOURCE IN THE ISSUANCE PROCESS.	55

## 12.4 Address change application



Skatteetaten

## Melding om ny/endret postadresse

Du trenger bare fylle ut de hvite feltene, de grå feltene er til intern bruk for skattekontoret.

Hvem kan levere dette skjemaet, og hvor kan det leveres?

**DU SOM IKKE SKAL FLYTTE, MEN BARE ENDRE POSTADRESSE**, kan fylle ut og levere dette skjemaet.

Du kan også levere skjemaet hvis du allerede har oppgitt en annen postadresse enn bostedsadressen til skattekontoret og ønsker å slette den, eller hvis du bor i utlandet og har endret postadresse der.

Dersom du skal flytte fra den bostedsadressen skattekontoret har registrert på deg, skal du **ikke** levere dette skjemaet, men melde flytting ved å bruke skjemaet *Flyttemelding – flytting innenlands*. Du skal sende meldingen om endret postadresse til et skattekontor eller levere den i skranken der. Adressen til ditt skattekontor finner du på skatteetaten.no.

**A** Hva slags endring gjelder meldingen?

Jeg/vi ønsker å registrere en ny postadresse. Gå videre til felt B.

Jeg/vi ønsker å slette den eksisterende postadressen og bare ha bostedsadressen registrert i folkeregisteret. Gå videre til felt C.

**B** Hva er den nye postadressen?

Adresse Øyvind Toftegaard [redacted] veien [redacted] [redacted] Oslo	Postnummer [redacted]	Sted Oslo
Land Norge		

**C** Hvem gjelder den endrede postadressen for?

I dette skjemaet kan du endre postadresse for bare deg selv, flere eller alle i husstanden.

Navn (etternavn, fornavn, ev. mellomnavn)	Fødselsnummer
1. Toftegaard, Øyvind Anders Arntzen	260582 [redacted]
2.	
3.	
4.	

**D** Hva slags legitimasjon legger du/dere ved meldingen om endret postadresse?

Jeg/vi legger ved:

kopi av pass

kopi av føreskort

kopi av et annet id-kort som inneholder fødselsdato, navn, signatur og bilde (NB! Ikke send kopi av bankkort.)

Du/dere som signerer meldingen, må legge ved kopi av gyldig legitimasjon. Gyldig legitimasjon er id-kort som inneholder fødselsdato, navn, signatur og bilde. Du/dere kan imidlertid ikke sende oss kopi av bankkort, fordi det inneholder sensitiv informasjon.

Hvis postadresseendringen gjelder hele husstanden, holder det med én underskrift og kopi av legitimasjon for den som signerer. Men hvis dere er flere som deler på foreldreansvaret for barn under 18 år, må den/de av foreldrene som barnet er registrert bosatt hos i folkeregisteret, signere meldingen og legge ved kopi av gyldig legitimasjon. Hvis du ønsker å endre postadressen på vegne av den du er verge for, må du dokumentere at du er oppnevnt som verge eller hjelpeverge. For dødsbo må skifteattest med eventuell fullmakt legges ved.

**E** Hvordan kan skattekontoret kontakte deg/dere?

E-postadresse oyvindat@mail.com	Telefon på dagtid 95820910
------------------------------------	-------------------------------

Melding mottatt (reg. dato)
-----------------------------

**F** Dato og underskrift

Dato 12/7-16	Underskrift(er) Øyvind Toftegaard
-----------------	--------------------------------------

Skattekontorets stempel og underskrift
--

RF-1454B

side 1/1



**12.5 Publishable paper derived from this master thesis work**



# An EoI Evaluation System

Øyvind A. Arntzen Toftegaard

Norwegian University of Science and Technology

**Abstract.** ID fraud is a serious problem which can be used to conduct crimes like economic fraud, human trafficking and terrorism. Many Norwegian organizations has pointed out challenges in performing ID control, and a national framework for ID proofing and verification is requested by Norwegian ID stakeholders. Internationally, there are already several guides and standards available for organizations on ID proofing and verification routines. However, complexity and variation among them can make them hard to interpret and understand, especially by smaller organizations performing ID control. At the same time, ID fraud seem to increase worldwide. This paper proposes an EoI evaluation system operationalizing requirements to EoI in ID proofing and verification processes. The suggested system is designed to be included in a computer application, allowing easy use by front-desk officers.

**Keywords:** Evidence of Identity, ID documents, ID proofing, ID verification.

## 1 Introduction

When you apply for a passport or inquire to loan a book at a library, an identity (ID) document is commonly used as Evidence of Identity (EoI). Based on the evidence a proofing party, being either the service provider itself or an ID proofing party, grant or decline access. EoI can be required to enroll a subject not previously known to the organization into an ID management system (ID proofing), or to determine whether a previously enrolled subject is the owner of the claimed identity (ID verification). ID documents include varying levels of security features. Typically, highly trusted EoI is required to access a high-risk service like for example opening a bank account or having a passport issued. On the other hand, loaning a book at a library can usually be done even with little EoI provided. Requirements to EoI may also differ depending on whether the subject is already enrolled in the organizations system or is applying for access to the service for the first time. Unlawful access to services associated with high risk could result in crimes such as terrorism, economic fraud and human trafficking.

ID fraud is a serious problem around the world. According to the American strategy and research company Javelin, ID fraud hit record high in 2016 with 15,4 million US victims and a cost of \$16 billion dollars [1]. In 2016, a fraud indicator report based on research by the University of Portsmouth, estimated annual ID fraud losses in the UK could be as much as £5,4 billion [2]. To counter ID related fraud, many nations and international organizations have developed frameworks in order to standardize ID evaluation and validation techniques. Examples on national frameworks are New Zealand's EoI standard related to online services and E-governance [3], Canada's standard on

identity and credential assurance [4], UK's national good practice guide on identity proofing and verification of individuals [5], Australia's guide for national identity proofing [6], and Norway's ID establishment guide (only at draft stage) [7]. Examples on global frameworks are the International Civil Aviation Organization's MRTDs – towards better practice in national ID management [8] and the ISO/IEC 29003 standard on identity proofing [9]. In addition, the EU research project ORIGINS [10] has provided recommendations on ID document standardization to the new standardization committee CEN/TC 224 WG 19 [11] established early 2017.

Many Norwegian organizations have described ID proofing as challenging, including the Norwegian Directorate of Immigration [12], the Norwegian Labour and Welfare Administration [13], the Norwegian Tax Administration [14], the Norwegian National Police [15], and the Norwegian ID (NID) Centre [16]. Norway has also seen ID fraud in many ways. Examples include illegitimate passport issuances made possible by a data migration error in the Norwegian National Registry [17,18,19], false Greek ID documents used as proof in a Norwegian court appeal during a divorce settlement [20,21], economic fraud based on registrations of fictive new-borns in the National Registry [22,23], and economic fraud based on use of multiple IDs from EEA-countries [24,25]. NID Centre published a report on ID fraud in 2015, showing 866 cases of ID document fraud were reported in Norway during 2014 [26]. ID document fraud seems to have increased over time, from 678 cases in 2012 and 787 in 2013 [27]. Already in 2013, the Norwegian ID Network, consisting of 14 Norwegian ID stakeholders, pointed out the need of a national ID proofing and verification framework [28].

Organizations performing ID proofing and verification have to interpret complex content of available frameworks. In addition, available frameworks deviate in content. A consequence could be EoI misjudgment due to content misinterpretations. One real-life example on such misjudgment is the ballot paper for the Norwegian parliamentary election of 2017. It stated that any ID document with the holder's name, birth date and picture could be used to vote [29]. This could allow use of digital ID documents on smartphones, corporation's access cards, and other ID documents which are difficult for election officers to be familiar with [30]. Since it is not likely that any front desk officer will be familiar with characteristics of all available EoI, this could be solved by either only requiring ID documents known by the officer, or by requiring combinations of ID documents. For the latter case, a computer application could calculate if the combined EoI of the subject provide a sufficient EoI level for access to the service offered by the front desk officer's organization.

The objective of this paper is to investigate and analyze the status of ID proofing and verification methodologies and attempt to operationalize the content of these frameworks into a more efficient EoI evaluation methodology. The proposed methodology should be possible to insert into a computer program, allowing it to be used by any organization performing ID proofing, regardless of knowledge by front desk officers.

This study is based on an extensive literature review, stretching from first data collections in 2015, until last literature searches in 2017. Sources were found based on I) online searches in the IEEE Xplore and Springer Link databases, II) sources recommended in meetings with employees of nine Norwegian ID stakeholder organizations,

and III) cooperation with the EU supported ORIGINS project (including fifteen European ID-stakeholders and research institutions).

While it seems to have been made quite some research on technical ID management like biometrics [31,32,33,34,35], less research is found on ID proofing and verification at policy level. Many of the sources used in this paper is from newspapers and non-scientific work such as guidelines and standards. The reason is that such sources can provide information not found in research papers at this point of time. Other research on EoI evaluation has described the same benefits and need of using such type of sources [36].

As this paper investigate characteristics, or qualities, that cannot be entirely reduced to numeral values, the methodic structure is based on recommendations for qualitative studies by Leedy and Ormrod [37]. At the same time, this paper also includes quantitative analyses of frameworks, and the proposed EoI evaluation system is a quantitative system allowing quantitative functionality testing in the future. This paper is structured like this: Section 1 introduces the challenges with use of current ID proofing and verification guides. Section 2 gives an overview of previous research efforts on EoI evaluation. Section 3 describes policies for an EoI evaluation system based on an examination of previous research. Section 4 describes an EoI evaluation system design, allowing easy EoI evaluation by front desk officers. Section 5 evaluates the EoI system's benefits and weaknesses. Section 6 concludes the paper and give recommendations for further research.

## 2 Previous work on EoI evaluation

### 2.1 Terms

Definitions are mainly based on the ISO/IEC 29003 standard on ID proofing [9]. It is used because ISO has a widespread portfolio of standards and it can be assumed the 29003 standard will be used by many parties in practice. Other sources are used where the ISO standard does not provide any definition.

**Identity proofing** – *“Process to verify identifying attribute(s) to be entered into an identity management system and to establish that the identifying attributes pertain to the subject to be enrolled”* [9].

**Verification** – *“A process performed to determine whether the Applicant is the owner of the claimed identity”* [5].

**Evidence of Identity** – *“Evidence that provide a degree of confidence that a subject is represented by the identity being claimed”* [9].

**Authoritative Evidence** – *“Holds identifying attribute(s) that are managed by an authoritative party”* [9].

**Corroborative Evidence** – *“Holds identifying attributes that are not managed by an authoritative party”* [9].

**Proofing information** – *“Information collected for identity proofing”* [9].

Note 1: Evidence of Identity can be ID documents, document databases, official records, an interview, a guarantor, own knowledge of the applicant, social footprint, biometrics, or a detailed life story [38].

Note 2: Authoritative Evidence could be both a corporation controlled database and an official registry. Corroborative Evidence may not be as up-to-date and accurate as Authoritative Evidence [9].

Note 3: An authoritative party is an entity that has the recognized right to create or record, and has responsibility to directly manage, an identifying attribute [9].

Note 4: Proofing information can be provided by either the subject or a reference [9].

## **2.2 Research from academia**

In 2004, Mason showed that a fabricated identity without an electronic biographic trial, can easily be created overnight [39]. Further, in 2008, Evans-Pughe showed that as more and more personal information is getting available online, personal data get its value as EoI reduced [40]. Also in 2008, Agbinya, Islam and Kwok published a study on a digital identity management system suggesting that use of multi-modal authentication will play a very big role in reducing cases of identity theft and fraud on online services [41]. In 2012, Wu et. al. proposed a personal identity management cycle model which could capture important events that happened around the management issues of a personal identity [42]. Then in 2013, Yang et. al. published a paper promoting standardization of EoI [36]. One of the conclusions by Yang et. al. was that multiple EoI databases should be available for data corroboration among each other to ascertain an identity's validity.

## **2.3 Research projects**

In 2012 the European Commission (EC) decided to finance the FIDELITY project [43]. It analyzed shortcomings and vulnerabilities in the ePassport life cycle, and recommended technical solutions and recommendations to overcome them. Most of the results are confidential. In 2015, EC also decided to fund the ORIGINS project [10]. It studied security levels of ID documents used in the passport issuance process, and gave recommendations to close security gaps in ID document systems within EU and Schengen. This project as well resulted in mostly confidential reports. From 2010 to 2011, FRONTEX performed a study on ePassport security [44], which concluded that national ID cards might be considered as a weak link due to lack of standardization. OSCE arranged a roundtable gathering on travel document security in 2013, concluding that civil registry systems are gaining international significance, and determine the level of trust in a country's travel document [45].

## **2.4 Standards and guidelines**

There have been many frameworks developed for ID proofing and verification processes. Already mentioned are the national and international standards and guides

[3,4,5,6,7,8, 9]. However, key objectives in ID proofing deviate between these sources. Taking ISO/ IEC 29003 [9] as a starting point, key objectives can be listed as follows:

- A:** To determine the ID is unique (duplication control)
- B:** To determine the ID exist (control against evidence that ID is not fictitious)
- C:** To determine the subject has some binding to the ID
- D:** To determine the ID is alive and in use (not belonging to a deceased)

In addition, two objectives not mentioned in ISO/IEC 29003, but mentioned by the UK's cabinet Office [5] and the Australian Attorney-General's Department [6] (**E**), and the Canadian Treasure Board Secretariat [4] (**F**) can be added:

- E:** To determine the ID is not used fraudulent (for example a blacklist control)
- F:** To determine the accuracy of the ID information

Table 1 show the objectives mapped to the previously mentioned standards and guides. Some objectives are mentioned in most guides indicating it is more important. Also, one guide and one standard cover fewer objectives than the others (The Norwegian and the Canadian). The question whether it means these are weaker can be raised. However, some discretion has been used by the author in the work of checking boxes, meaning the reliability of the results of mapping guides and standards to key objectives can to some degree be discussed.

**Table 1.** How key objectives in ID proofing and verification are covered in a selection of guides and standards. The key objectives are derived from all the selected standards and guides (**X** = guide or standard cover the objective. **/** = guide or standard partly cover the objective).

Selected sources of key objectives in ID evaluation	Key objectives proposed by sources					
	A	B	C	D	E	F
<b>International Organization for Standardization</b> ISO/IEC 29003 – Identity proofing [9]	X	X	X	X		
<b>International Civil Aviation organization</b> Towards better practice in national ID management [8]	/	X	X	X		
<b>New Zealand Department of Internal Affairs</b> Evidence of identity standard [3]	/	X	X	X		
<b>Canadian Treasure Board Secretariat</b> Standard on Identity and Credential Assurance [4]	X		X			X
<b>UK's Cabinet Office</b> Identity proofing and verification of an individual [5]	X	X		X	X	
<b>Australian Attorney-General's Department</b> National Identity Proofing Guidelines [6]	X	X	X	X	X	
<b>Norwegian ID Network (draft stage)</b> Guide for ID establishment of physical persons [7]	X	X	X			

### 3 Proposing policies for a quantitative EoI evaluation system

In Table 1 objective A, B, C and D are mentioned most, indicating they are most important. In addition, the UK [5] and Australian frameworks [6] includes a control of ID against fraudulent use (objective E). This could be done fast if there is digital access to a blacklist or similar, and should therefore also be considered. When it comes to the Canadian standard's [4] objective to determine accuracy of ID information, it refers to either ID control against an authoritative source or ID inspection by a trained examiner. It can be argued that control against authoritative sources already will be covered by previous listed objectives. Further, manual inspection by a trained examiner can be seen as too time consuming for a universal methodology, where any front desk officer should be able to perform the ID control. A short inspection should be performed, but it is unlikely that a thorough inspection will be performed by a front desk officer. Therefore, the following work will only put weight on key objective A – E from previous chapter. According to ISO/IEC 29003 [9], EoI typically includes one or more of the following:

- I) Proofing information provided by the subject
- II) Issued evidence containing or linking to subject proofing information
- III) Databases and registers containing subject proofing information
- IV) Proofing information provided by other known sources

For simplicity reasons, this paper proposes to calculate EoI value of all types of EoI's in one process, including both Authoritative Evidence, Corroborative Evidence and Proofing Information. An algorithm, proposed for the first time in this report, can be used to calculate an accumulative EoI level value. The algorithm will cover the objectives of determining whether an ID is unique, that it exist, that there is a binding between the subject and the claimed ID, and that the ID is in use. Thereby, this proposal shall provide trust in ID proofing and verification processes at level with main objectives of previous guides and standards presented in this paper, and especially the ISO/IEC 29003 standard [9]. For EoI checking, the ISO standard recommends:

- |                             |                                      |
|-----------------------------|--------------------------------------|
| I) Physical evidence checks | III) Verification with issuing party |
| II) Binding to subject      | IV) Corroboration                    |

The EoI evaluation system proposed in this paper will cover step I, III and IV in one part-calculation, where both Corroborative and Authoritative Evidence, and their interactions, will be evaluated. Thereafter, any binding between available evidence and the subject shall be controlled. This can be done electronically by the use of biometrics, or manually in form of an interview with the subject or a reference person.

In this work, two weaknesses have been found in the ISO/IEC 29003 standard [9] when it comes to ID proofing and verification: I) It assume that a false or tampered ID document can be detected. That is not always the case, for example many countries do not have registers of all formats of old birth certificates. II) It does not make a separation between Physical Personal ID documents and Digital Personal ID documents, even though requirements to such ID documents can be quite different.

This paper proposes to divide Corroborative Evidence in 2 sub-categories: I) **Digital Personal type ID documents (DPID)** – for example a digital student ID, a web-based

public eID, or content of an e-mail or facebook account, and II) **Physical Personal type ID documents (PPID)** – for example a passport, driving license, bank card, birth certificate, or tax certificate. Further, this paper proposes to define Authoritative Evidence as **Digital Reference type ID documents (DRID)**. A DRID could for example be a driving license registry, a passport registry or a civil registry. This way both Authoritative and Corroborative evidence can be fitted into 3 subcategories which can be used to estimate EoI in the proposed EoI evaluation system.

#### 4 Finding EoI values and using them for EoI evaluation

EoI values of 1, 2 and 3 for ID documents (DRID, DPID and PPID), and 1, 2, 3, 4 and 5 for binding to subject, were chosen in this paper for simplicity reasons. According to ISO/IEC 29003 [9] strength of EoI will come from three aspects:

- A) The original identity proofing undertaken
- B) The process used to issue it
- C) The quality and robustness of the security features to prevent tampering, counterfeiting and forgery

In addition to these, this paper propose to add three more aspects:

- D) Accountability/risk of prosecution
- E) Organizational measures
- F) Available information to bind subject to ID document

If ID fraud would result in prosecution (due to traceability) EoI strength would increase. Traceability is a key aspect in information security. In addition, organizational security measures are gaining more focus, often connected to the ISO/IEC 27001 information security management system standard [46]. Last, it will be a need of available information to bind subject to the ID document. All these aspects are very transferrable to both DRID, DPID and PPID. From now on, when only the term “ID document” is used, it means all ID document types (both DRID, DPID and PPID).

##### 4.1 EoI value requirements for ID documents

Table 2 shows how ID documents are mapped to EoI values. Acknowledging the value of a linkage between an ID document and a reference system, EoI value for DRID is added to EoI value of PPID or PDID as shown in subchapter 4.3.

**Table 2.** Requirements for ID documents. Letters at the left represents which of the EoI strength aspects above (chapter 4) the requirement mainly relates to.

Requirements which if all fulfilled gives EoI value 1	
1.(A)	It must not be possible to be enrolled in DRID or having issued PPID or PDID without any form of authentication (document accessibility)
2.(C)	The ID authority (for DRID, DPID, or PPID) must have some kind of mechanism to prevent unauthorized change of ID information (integrity)
3.(D)	It must be possible to hold one organization liable for ID document security breaches (traceability)
4.(F)	The ID document must present a unique ID in the application context, such as name, email address, social security number, etc.

Requirements which if all fulfilled gives EoI value 2	
1.	Point 2 - 3 in requirements EoI value 1 must be fulfilled
2.(A)	It must not be possible to be enrolled in DRID or having issued PPID or PDID without strong authentication (document accessibility)
3.(B)	An issuing party of DPID and PPID shall have a delivery process securing that ID documents will be delivered only to the correct person
4.(C)	Any ID document must include security elements providing moderate to high protection against fraud
5.(D)	Any ID registration shall be traceable to one employee at the EoI issuer
6.(D)	The rights to production and personalizing of any ID document shall be protected and reserved one special organization
7.(E)	An ID document issuing party shall have available routines concerning the application process and the production/personalization of the ID document
8.(E)	An issuing party of DPID and PPID shall have documented routines and processes for registering and reporting lost and stolen ID documents (fraud control)
9.(F)	The ID document must as a minimum contain: -Holders full name and date of birth -A unique reference number or ID number -Face portrait or other biometrics with equivalent or better accuracy
Requirements which if all fulfilled gives EoI value 3	
1.	Point 1 - 9 in requirements EoI value 2 must be fulfilled
2.(A)	There must be a control against duplicate identities as part of any ID establishment process, concerning; A) Information already exists, and B) Biometrics already exist
3.(E)	The responsible party shall have routines for periodically audits of all ID's registered
4.(E)	The responsible party shall have documented routines concerning the whole life cycle of the ID document in line with ICAO's best practice or at similar level

#### 4.2 EoI value requirements for binding to subject

A strong link between an ID document and the subject can augment an EoI value derived unilateral from the ID document part. Requirements for EoI values associated with a single binding to subject, is suggested in this paper as follows:

**Table 3.** Requirements for binding to subject

	Manual Biometric match	Electronic Biometric match	Password or token corresponds	Interview corresponds	Written declaration corresponds
DPID EoI 1	EoI value 1	EoI value 1	EoI value 1	N/A	N/A
PPID EoI 1	EoI value 1	EoI value 1	EoI value 1	N/A	N/A
DRID EoI 1	EoI value 2	EoI value 2	EoI value 1	N/A	N/A
DPID EoI 2	EoI value 2	EoI value 2	EoI value 1	N/A	N/A
PPID EoI 2	EoI value 2	EoI value 2	EoI value 1	N/A	N/A
DRID EoI 2	EoI value 3	EoI value 3	EoI value 1	N/A	N/A
DPID EoI 3	EoI value 3	EoI value 4	EoI value 1	N/A	N/A
PPID EoI 3	EoI value 3	EoI value 4	EoI value 1	N/A	N/A
DRID EoI 3	EoI value 4	EoI value 5	EoI value 1	N/A	N/A
ID in general	N/A	N/A	N/A	EoI value 2	EoI value 3



As can be seen in table 3, there are possibilities to achieve an EoI value even without any ID document. Either through an interview, or through a reference person. Electronic biometric matches with physical ID documents must for security reasons only be based on an onboard chip or similar protected infrastructure. A biometric match for the same ID document should only be counted one time. For example, the EoI value from a manual biometric match should not be added to the EoI value from an electronic biometric match for the same ID document. The reason is that it will not give extra EoI when the binding is already confirmed at a higher level.

#### 4.3 Calculating EoI level value based on multiple evidence and multiple bindings to subject – a methodological approach

Combinations of ID documents in the proposed scheme will only add 50% of the value of the next additional document, resulting in a negative exponential function. This avoids that two ID documents with the same EoI value are considered twice as secure as one ID document, as would be the case by using a linear function (Figure 1 A). Further, the negative exponential function will acknowledge the value of the first document unlike use of a positive exponential function (Figure 1 B). It will also avoid situations where many ID documents with low EoI value are combined to reach a high final EoI value without being bound with an upper limit (Figure 1 C and D). The first part of the calculation algorithm:

$$P = D_1 + 2 \sum_{i=2}^N \frac{D_i}{2^i} \quad (1)$$

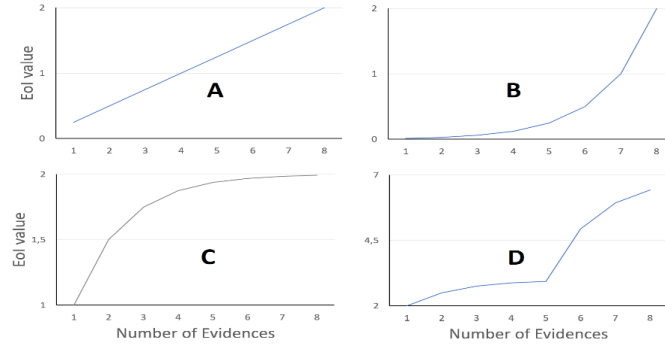
Where P is the *EoI Part value* resulting from this calculation, and D is the individual *ID Document's EoI value*. Note that Eq.(1) is a convergent series so that the value P can be bound to a value which can be used to thwart the attempt to combine multiple low-EoI-value evidences to reach a high EoI value. In order to acknowledge the values of ID documents with high EoI values, these should be placed first in the algorithm. For example, D<sub>1</sub>: Passport, D<sub>2</sub>: Driving License, D<sub>3</sub>: Birth certificate. Now, EoI values for the binding to subject should be calculated and added separately to P, in a final EoI value calculation:

$$V = P + (B_1 + 2 \sum_{i=2}^N \frac{B_i}{2^i}) \quad (2)$$

Where B is EoI values of **Bindings to subject**, and V is the *EoI level Value* used to map the combined EoI to the EoI level it corresponds to.

Figure 1 C show that even if multiple ID documents at EoI value 1 will not allow the achievement of the next EoI value. This is an advantage as these documents are so easy to forge. However, any document with higher EoI value, or a binding to subject, will depending on its value, allow to climb several EoI values (Figure 1 D). This system successfully stops attempts on use of multiple low-value ID documents or bindings to climb in the EoI hierarchy. The main advantage with the algorithm is that it gives such clear thresholds for what a subject can achieve with combined EoI of different values.

**Fig. 1.** Characteristics of possible EoI value calculation methodologies: A: Characteristics of a linear function, B: Characteristics of a positive exponential function, C: Example of negative exponential function as proposed in this paper (using multiple ID documents at EoI value 1), and D: Example of negative exponential function as proposed in this paper (using one ID document with EoI value 2, four with EoI value 1, and three bindings to subject with EoI value 2).



#### 4.4 Mapping EoI level value to corresponding EoI levels

Calculation of an EoI level value could for example look like this: EoI level Value = Passport + (Manual biometric match of subject to PPID with EoI value 2 + Interview) equals  $V = D_1 + (B_1 + 2 * (\frac{B_2}{2^2}))$  equals  $V = 3 + (2 + 2 * (\frac{2}{4}))$  equals EoI level Value = 6. ISO/IEC 29003 [9] suggest use of 3 EoI levels (levels of identity proofing): low, moderate and high. However, in the ISO standard, the levels are based on qualitative evaluations. Three levels can also be used to map EoI level values found by quantitative techniques in this paper to EoI levels as seen below. The thresholds are chosen based on the functions and the content of the proposed algorithm. The design assures that multiple ID documents with EoI value 1 cannot be used to gain access to services at EoI level moderate. It also assures that EoI level high in practice is unreachable without both an ID document and a binding to subject where both offer a high EoI value.

<b>EoI level low</b> (EoI level value < 2)	< equals less than
<b>EoI level moderate</b> (EoI level value $\geq 2$ and < 6)	$\geq$ equals larger or equal to
<b>EoI level high</b> (EoI level value $\geq 6$ )	

#### 4.5 The full EoI evaluation system

An infrastructure model illustrating core elements of the proposed EoI evaluation system is displayed in figure 1. The officer at the counter must decide if the necessary EoI level have been reached for the service applied for (for example to have a bank card issued). This evaluation process can be done with a high degree of automation through the unique EoI evaluation system proposed in this paper. The proposed EoI evaluation system will cover all ID proofing steps as described in ISO/IEC 29003 [9]:

- I) Collect the proofing information
- II) Determine the veracity of the evidence collected against objectives

- III) Determine that identifying attributes from the EOI meet the required EoI level  
 IV) Bind the subject to the claimed identifying attributes

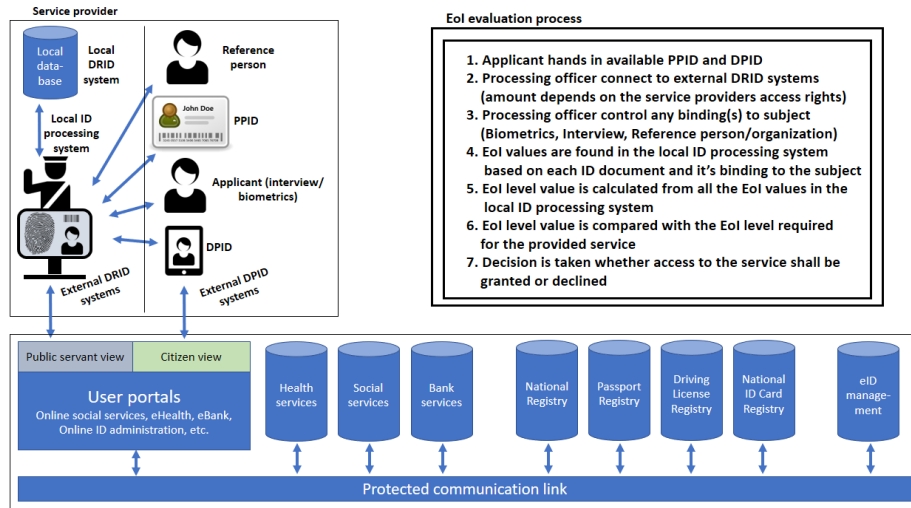


Fig. 2. EoI evaluation infrastructure of the EoI evaluation system proposed in this paper.

## 5 Discussion

Evidence fulfilling requirements of EoI value 1 would typically be a birth certificate, content of a facebook account, or a database registration at a library. Such evidence has a low value as EoI since they are easy to falsify and difficult to validate. Evidence fulfilling requirements of EoI value 2 would typically be a bank card with picture of the holder, or a driving license registry registration. Such evidence provides more value as EoI since they contain more security features. As an example, physical driving licenses (EU type) have security features like holographic print, relief-pattern, UV print and IR features [47], in contrast to the Norwegian birth certificates which usually only contain safety features like signature and stamp of document issuer. Evidence fulfilling requirements of EoI value 3 would typically be a passport, or an immigrant registry registration. Such Evidence are characterised by security features at a national level, including digital features, since security breaches could cause severe consequences.

EoI values proposed by the author in this paper are based on an extensive literature survey and meetings with nine ID stakeholders in Norway. There is a chance that some EoI have been given wrong values. For example, different levels of accuracy could exist between ID related information. This is covered by the UK's EoI guide [5], but it is not reflected in this proposal. The reason is that it is assumed to be too time consuming to investigate all provided EoI thoroughly. At the same time, the UK guide was the only one addressing this area from seven different guides, indicating the importance could be considered low. Still, this might be an area which should be investigated more in the future.

The quantitative EoI evaluation system proposed in this paper can be used in processes of deciding whether EoI provided by an applicant is at corresponding level with security requirements of the service provided by the organization. Characteristics of the EoI evaluation algorithm proposed in this paper are in line with recommendations for use of multiple EoIs [36,39,41,42]. In addition, human factors such as uncertainty regarding choice of EoI level might be less present in a quantitative system compared to one based on qualitative evaluation. By pre-defining EoI belonging to each EoI value, organizations will no longer have a challenge in choosing which EoI to ask for in order to give access to their service. Such pre-definition should preferably be performed at a national level, and harmonized across Europe, assuring equality in EoI requirements between similar services.

Manual biometric matches have been given lower EoI values than electronic matches in this proposal. This is because existing research work show indications that automatic face recognition technology provides better results than manual face comparison [48,49]. Further, a written declaration is given a quite high EoI value, since EoI requirements then, to a certain degree, can be transferred to the liable reference person who had already established trust from a proofing party.

Uncertainty in the proposed EoI evaluation system will mostly be connected to in which degree correct requirements have been set in table 2 and 3 of this paper. Requirements in this paper are mostly inspired by other nation's guides and standards. At the same time, the introduction of DPID complicates the process of choosing requirements. Use of main elements from ISO/IEC 29003 [9] ensures reliability of the main principles of EoI evaluation used in this work. If any organization would be willing to use this system for a time period, it could further validate its effect.

## **6 Conclusion and recommendations for further research**

The methodology for EoI evaluation presented in this paper can be used to assign different EoI appropriate EoI values. Further, by the use of an algorithm, their combined EoI value can be mapped to a functional EoI level. ISO/IEC 29003 [9] focuses on ID uniqueness, existence and whether the subject has a strong binding to the ID. The unique EoI evaluation system proposed in this paper provides trust in ID establishment and verification processes at level with main principles of the ISO standard, as well as most other ID guides and standards presented in this paper. The work laid down in this paper show how these principles can be operationalized and fed into a quantitative system for easier and faster EoI evaluation.

This paper has proposed a ready-to-test EoI evaluation system. In the future, developing an application allowing real-life testing of the proposed EoI evaluation system, would be a natural next step. It is hard to estimate the presumable effect of the proposed EoI evaluation system, since it has not been tested in practice. As testing of such a system would be time consuming and cooperation demanding from different stakeholders, this limited work has focused on developing a system model instead of testing its performance in operation. This leaves it to any interested party to test the system in practice over a time period in order to evaluate its performance.

## Acknowledgements

Great thanks to Bian Yang (NTNU), Magnar Aukrust and Janne Hagen for support in the process of writing this paper.

## References

Bibliography structure is based on Springer Basic Style [50].

1. Javelin (2017) Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study. <https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new>. Accessed 9 Sep 2017
2. Experian, PKF Littlejohn and the University of Portsmouth's Centre for Counter Fraud Studies (2016) Annual fraud indicator. <http://www.port.ac.uk/media/contacts-and-departments/icjs/ccfs/Annual-Fraud-Indicator-2016.pdf>. Accessed 9 Sep 2017
3. New Zealand Department of Internal Affairs (2009) Evidence of Identity Standard. <https://www.dia.govt.nz/Resource-material-Evidence-of-Identity-Standard-Index>. Accessed 19 Feb 2017
4. Canadian Treasury Board Secretariat (2013) Standard on Identity and Credential Assurance. <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776>. Accessed 19 Feb 2017
5. UK's Cabinet Office (2014) Identity proofing and verification of individual. <https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual>. Accessed 19 Feb 2017
6. Australian Attorney-General's Department (2016) National Identity Proofing guidelines. <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/NationalIdentityProofingGuidelines.PDF>. Accessed 19 Feb 2017
7. Norwegian ID Centre (2016) Veileder i fastsettelse av identitet til fysiske personer. Norway, Oslo (in press)
8. International Civil Aviation Organization (2013) Machine readable travel documents – towards better practice in national identification management. <https://www.icao.int/Security/mrtd/Documents/TR%20-%20%20EOI%20Version%20Release%203%20Draft%2030%20April%202013.pdf>. Accessed 16 May 2016
9. International Organization for Standardization (2016) ISO/IEC DIS 29003 Information technology – Security techniques – Identity proofing 2016-11-07
10. ORIGINS (2015) Recommendations for Reliable Breeder Documents. <http://www.origins-project.eu/>. Accessed 28 Feb 2017
11. Standard Norge (2017) Én grunnleggende identitet. <https://www.standard.no/nyheter/nyhetsarkiv/ikt/2017/en-grunnleggende-identitet/>. Accessed 9 Sep 2017
12. De Rosa I (2015) UDI: Politiets ID-kontroll bør bli bedre. Available via the Norwegian Broadcasting Corporation. [https://www.nrk.no/norge/udi\\_-\\_politiets-id-kontroll-bor-bli-betere-1.12718659](https://www.nrk.no/norge/udi_-_politiets-id-kontroll-bor-bli-betere-1.12718659). Accessed 7 Sep 2017
13. Fladby M (2009) ID utfordringer for NAV. Available via Slideshare. <https://www.slideshare.net/Utlendingsdirektoratet/udis-vrkonferanse-2009-id-utfordringer-for-nav>. Accessed 7 Sep 2017
14. Remen AC, Reinholdtsen L (2016) Skattedirektøren: ID-sjekk av utlendinger er for dårlig. Available via the Norwegian Broadcasting Corporation. <https://www.nrk.no/norge/sjekker-ikke-id-godt-nok-1.12794326>. Accessed 7 Sep 2017

15. Rørslett K, Brekke A (2013) Klarer ikke å sjekke falsk ID. Available via the Norwegian Broadcasting Corporation. <https://www.nrk.no/norge/klarer-ikke-a-sjekke-falsk-id-1.11370176>. Accessed 11 Sep 2017
16. Norwegian ID Centre (2014) Kartlegging av ID-arbeid. <https://www.nidsenter.no/globalassets/vedlegg/nid-rapporter/evaluering---del-2.pdf>. Accessed 7 Sep 2017
17. Oppegård GG (2012) Nekter for at utlendinger urettmessig er blitt norske statsborgere. Available via TV2. <http://www.tv2.no/a/3871926/>. Accessed 28 Jul 2017
18. VG News (2012) 58.000 utlendinger registrert som norske statsborgere etter datatabbe. <http://www.vg.no/nyheter/innenriks/58-000-utlendinger-registrert-som-norske-statsborgere-etter-datatabbe/a/10068558/>. 28 Jul 2017
19. Haakaas E (2012) 58.000 utlendinger ble norske etter datatabbe. Available via Aftenposten. <https://www.aftenposten.no/norge/58000-utlendinger-ble-norske-etter-datatabbe-144878b.html>. Accessed 28 Jul 2017.
20. Hansen S, Kristoffersen EB, Vaglieri M (2015) Passmannen. Available via the Norwegian Broadcasting Corporation. <http://www.nrk.no/dokumentar/xl/passmannen-1.12404097>. Accessed 27 Feb 2016
21. Widerøe RJ, Tommelstad B, Andersen G et al (2016) Slik lot NRK seg lure. Available via VG. <http://www.vg.no/nyheter/innenriks/geir-selvik-malthe-soerenssen/slik-lot-nrk-seg-lure/a/23641960/>. Accessed 28 Jul 2017
22. Holm PA, Dragland LL (2011) Fikk millionstøtte til barn som ikke eksisterte. Available via Aftenposten. <http://www.aftenposten.no/nyheter/iriks/Fikk-millionstotte-til-barn-som-ikke-eksisterte-6667444.html>. Accessed 10 Sep 2015
23. Johansen PA (2013) Har slettet 70 falske barn i Folkeregisteret. Available via Aftenposten. <http://www.aftenposten.no/nyheter/iriks/Har-slettet-70-falske-barn-i-Folkeregisteret-7118493.html>. Accessed 10 Sep 2015
24. Remen AC, Reinholdtsen L (2016) Skattedirektoratet: -Letttest å lure seg inn i Norge med falske EØS-papirer. Available via the Norwegian Broadcasting Corporation. <https://www.nrk.no/norge/falske-eos-borgere-en-storre-trussel-enn-falske-asylsokere-1.12796161>. Accessed 28 Jul 2017
25. Dragland LL, Haakaas E (2014) Snekker med syv falske navn svindlet Nav for over en halv million. Available via Aftenposten. <https://www.aftenposten.no/norge/i/oRr0K/Snekker-med-syv-falske-navn-svindlet-Nav-for-over-en-halv-million>. Accessed 17 Aug 2017
26. Norwegian ID Centre (2015) Misbruk av ID-dokumenter 2014. [https://www.nidsenter.no/Global/Publikasjoner/NID\\_Brosjyre\\_2014\\_web\\_endelig.pdf](https://www.nidsenter.no/Global/Publikasjoner/NID_Brosjyre_2014_web_endelig.pdf). Accessed 21 Mar 2016
27. Norwegian ID Centre (2014) Misbruk av ID-dokumenter 2013. [https://www.nidsenter.no/Global/Publikasjoner/misbruktedokumenter\\_2013.pdf](https://www.nidsenter.no/Global/Publikasjoner/misbruktedokumenter_2013.pdf). Accessed 21 Mar 2016
28. National ID Centre (2013) ID-nettverkets bakgrunn. [https://www.nidsenter.no/fag/inholdside\\_id-nettverket/inholdside-om-opprettelsen/](https://www.nidsenter.no/fag/inholdside_id-nettverket/inholdside-om-opprettelsen/). Accessed 7 Sep 2017
29. Valgdirektoratet (2017) Stortings- og sametingsvalget 2017. <https://valg.no/globalassets/dokumenter/valgmateriell/informasjonsbrosjyrer/valgbrosjyre-bokmal.pdf>. Accessed 3 Sep 2017
30. Lien ØF (2017) - Uklare krav til id-kontroll. Available via Oppland Arbeiderblad. <https://www.oa.no/valg2017/informasjossikkerhet/ntnu-i-gjovik/uklare-krav-til-id-kontroll/s/5-35-487432>. Accessed 12 Sep 2017
31. Yang C (2014) Fingerpring biometrics for ID document verification. Industrial electronics and applications: 1441-1445
32. Paunwala MC, Patnaik S (2010) Sheltered Identification with Hiding Biometrics. Signal and Image Processin: 191-196

33. Fairhurst MC (2003) Document identity, authentication and ownership: the future of biometric verification. IEEE Conference Publications: 1108-1116
34. Thein HH, Sein MM, Aung SNL (2007). A reliable technique for personal identification or verification. IEEE Conference Publications: 265-269
35. Elliott SE, Massie SA, Sutton MJ (2007) The Perception of Biometric Technology: A Survey. IEEE Conference Publications: 259-264
36. Yang B, Busch C, Bringer J et al (2013) Towards standardizing trusted evidence of identity. Proceedings of the 2013 ACM workshop on Digital identity management: 63-72
37. Leedy P, Ormrod JE (2013) Practical Research – Planning and design. USA, Pearson
38. International Civil Aviation Organization (2010) Guide for assessing security of handling and issuance of travel documents. <https://www.icao.int/jahia/webdav/shared/shared/mainsite/activities/tcm/Assessment-Guide-PART1-Best-Practices-Jan-2010.pdf>. Accessed 16 May 2016
39. Mason S (2004) Validating identity for the electronic environment. IET Conference Publications: 54-70
40. Evans-Pughe C (2008) A crisis of identity. Engineering & Technology: 16-18
41. Agbinya JI, Islam R, Kwok C (2008) Development of digital environment identity (DEITY) system for online access. Third International Conference on Broadband Communications, Information Technology & Biomedical Applications: 1-8
42. Wu L, Ping R, Donghong S et al (2012) Research in techniques of personal identity management. IEEE Conference Publications: 912-915
43. FIDELITY (2012) About FIDELITY. <http://www.fidelity-project.eu/>. Accessed 16 May 2016
44. European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (2011) Operational and technical security of electronic passports. [http://frontex.europa.eu/assets/Publications/Research/Operational\\_and\\_Technical\\_Security\\_of\\_Electronic\\_Pasports.pdf](http://frontex.europa.eu/assets/Publications/Research/Operational_and_Technical_Security_of_Electronic_Pasports.pdf). Accessed 16 May 2016
45. Organization for Security and Co-operation in Europe (2013) Addressing the link between travel document security and population registration/civil registration documents and processes. <http://www.osce.org/secretariat/110610?download=true>. Accessed 16 May 2016
46. International Organization for Standardization (2013) ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems - Requirements
47. The Norwegian Public Roads Administration (2013) Nytt norsk førerkort fra 19. januar 2013. [https://www.vegvesen.no/\\_attachment/493459/binary/801365?fast\\_title=Nytt+f%C3%B8rerkort+19.+januar+2013+-+brosjyre.pdf](https://www.vegvesen.no/_attachment/493459/binary/801365?fast_title=Nytt+f%C3%B8rerkort+19.+januar+2013+-+brosjyre.pdf). Accessed 2 Sep 2017
48. White D, Kemp RI, Jenkins R et al (2014) Passport officers' errors in face matching. Available via NCBI. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4136722/pdf/pone.0103510.pdf>. Accessed 14 May 2017
49. Opitz A, Kriechbaum-Zabini A (2015) Evaluation of face recognition technologies for identity verification in an e-gate based on operational data of an airport. International conference on advanced video and signal based surveillance: 1-5
50. Springer (without year) Key style points: References Springer Basic Style. [http://www.springer.com/cda/content/document/cda\\_downloadocument/Key\\_Style\\_Points\\_BasicRef.pdf?SGWID=0-0-45-1330668-0](http://www.springer.com/cda/content/document/cda_downloadocument/Key_Style_Points_BasicRef.pdf?SGWID=0-0-45-1330668-0). Accessed 11 Sep 2017