Security Issues in ePassports

- ICAO Standard and National Implementations as Part of the US Visa-Waiver Program

by

Eili Bjelkåsen
Linda Walbeck Olsen

Thesis in partial fulfilment of the degree of
Master in Technology in
Information and Communication Technology

Agder University College
Faculty of Engineering and Science

Grimstad
Norway

May 2006

Abstract

After the 9/11 terror attacks against the US there have been concerns about how to positively identify every individual entering a country. As a direct result ePassports are now being issued in several countries all over the world. The International Civil Aviation Organization (ICAO) has developed the internationally applied standard for ePassports. The ICAO standard provides a guideline for what features that could or should be implemented in these passports. During the process of updating the standard several experts within security and privacy have argued that the standard is to weak.

The ePassports include biometrics and other personal information on a RFID chip. The fact that the information is now available on an RFID chip provides more security concerns than if the information had only been available in the machine-readable zone and at the data page. The chip itself provides some possible security and privacy problems like issuance, encryption, read range and so on, but there are also other aspects to consider with implementation of RFID.

If RFID is implemented it is very likely that a national or international database containing personal information about passport holders will also be implemented. This is because it is easier and faster to check travel history, criminal records and so forth if the passport is electronic crosschecked against the database. In addition, it will greatly increase the difficulty of passport fraud. If this database is to be implemented it is highly important that the security around it is the best it can be.

In our studies we have found that the continuous work with the ICAO standard for Machine Readable Travel Documents will probably give a thorough revised and considered result. Even though we find it somewhat disturbing that there are so many aspects brought to the group's attention by other security and privacy experts.

As the US has pushed for use of biometrics in passports through the US VISA-Waiver Program, more and more countries find it useful to implement biometrics. Biometric features in passports will give a fairly accurate identification rate; especially if the applied biometric is fingerprints or iris scan. All ICAO members have to implement Machine Readable Passports (MRPs) by 2010, and we believe that many of these countries, if not all, will enhance it with biometrics in that period of time.

Foreword

This report includes an analysis of the new biometric passport system, which is implemented in large parts of the world. The idea behind the report was to look at the security aspects facing such a big implantation as the ePassport system is.

The project, which this report is a part of, is a part of the Master degree in Information and Communication Technology at Agder University College – Faculty of Technology. The project is accomplished in Arendal and Grimstad. The report will be of interest for anybody that is interested in security and the new ePassports, but some experience in the field of Information and Communication Technology would be beneficial.

We give our sincere thanks to our supervisor Ola Torkild Aas for guidance through the project. We would also like to give our thanks to Atle Årnes at the Norwegian Data Inspectorate for providing us with quick and helpful answers to our questions.

Grimstad, May 2006.
Eili Bjelkåsen and Linda Walbeck Olsen

Table of Contents

List of Figures

1 Introduction

1.1 The Problem

1.1.1 Statement of the problem

Our study discusses whether the first generation of the new, biometrical passports are secure enough, from the governments' perspective. The main focus is on the International Civil Aviation Organization (ICAO) standard [1], which is used in some form by all countries that are part of the US Visa-Waiver program (VWP) [2]. If we find vulnerabilities in the standard or selected implementations thereof, we will if possible describe existing methods to eliminate, or at least improve these.

1.1.2 Sub problems

The first sub problem is to determine the quality of the ICAO standard, and evaluate the technical and practical solutions presented in the document. One problem immediately comes to attention: What is 'secure enough'? The literature on security often describes algorithms that theoretically could be broken, but are complex enough to be computationally infeasible to break, as 'secure enough'. This will be our starting point in describing what is secure, what is not secure and what is secure enough. (This problem itself can be divided into several sub problems, such as: The relationship between security and privacy; the security issues in the applied technology; the possible use and properties of an international control network; the growing concerns of the privacy-affiliated organizations and individuals all over the world; and the danger of possible fraud or forgery. We cannot effectively study all of these issues in detail, due to the limited time available. Instead, we will take a shallower look at all of them.)

The second sub problem is to present and evaluate possible solutions to weaknesses we might find in the ICAO standard.

The third sub problem is to view the implementation of the ICAO standard by chosen governments in search for differences that may or may not influence the quality of the international system. We will mainly focus on the US and Norwegian electronic passport, for several reasons. First, the US ePassport programme is one of the most public ones we have seen. The process of making US ePassports has been going on for some time, and has been easy to follow. We have seen several security and privacy issues publicly debated, and solutions have been devised. Also, the US is the country to begin the process of electronic passports, and is the first to require electronic passport from visitors.

The Norwegian ePassport programme is clearly interesting to us as we are, obviously, Norwegian. In addition, Norway is the third European country (only beaten by Belgium and Sweden) to issue the ePassport, and is therefore one of the pioneering countries in the ePassport context. Norway is to some extent required to follow EU guidelines, but also has opportunity to make many of its own decisions. It is unknown how much information is available on the Norwegian program, so other countries' passport implementations may be added. The new Scandinavian passports are, or will be, developed by the Finnish company Setec, so this company may become a source of information regarding the specifications of the Scandinavian electronic passports [3].

The fourth sub problem is to sum our findings, and determine as best we can whether the new electronic passports really are secure enough. Based on this, we can also try to recommend a minimum implementation that eliminates the most critical problems, if any.

1.1.3 Hypotheses

Our first hypothesis is that the ICAO standard has some weaknesses, but that it is possible to eliminate or improve these, although probably at an increased financial cost.

The biometrical passports are being implemented to combat forgery, among other reasons. Forgery, we claim, may however still be possible, especially if no particular measures are taken to ensure security.

We also believe that the RFID-technology might still be too young and weak to be a completely secure means of making passports (partly) digital.

The final hypothesis is that the different implementations of the governments can create new, previously undiscovered problems.

1.1.4 Delimitations

- We will not attempt to forge a biometric passport.
- We will not try to discover and solve all problems concerning biometric passports.
- We will not write a new standard for biometric passports
- We will not discuss all implementations of biometric passports, only a selected few. (i.e. the Norwegian and US implementations).
- We will not make a detailed study of the biometric passports technologies.

1.1.5 Definition of Terms

'**Biometric passport**': The new type of passports, which from October 2006 are required for entry to the US by the VWP. The passports must contain an RFID-chip, which holds digitized information about the passport's owner. The individual government decides much of the specific digital information, but certain demands are made by the US and the ICAO standard. As an example, a digitized photo of the passport's owner is required both by the standard and by the US. Some of the information on the passport must also be optically readable. Other terms used include 'electronic' or 'digitized' passports, or simply E-passports or ePassports.

'ePassport': A term used for all passports that includes an electronic device, or Contactless Integrated Circuit (IC) such as a RFID chip. The RFID chip contains biometric data, so an ePassport is also a biometric passport. This definition is in compliance with the ICAO terminology.

'**Standard**': A specification of procedures, technologies and other implementations of a principal. Used to ensure compatibility between different vendors, securing functionality, security, privacy and other features. A standard can be well established or it may not. The ICAO standard is a 'de facto' standard, meaning it is not yet ratified, but as there is no other, better standard, it is used. It may very well be ratified in the near future. The ISO standards, however, are ratified and well established.

'**Duplex**': Two-ways, in IT terminology normally used to indicate that communication is going both ways between two interacting entities.

'**Scandinavia**': The three neighboring countries Norway, Sweden and Denmark.

'**Skimming**': An unauthorized read of information, in our case from an RFID chip.

'**Faraday Cage**': A capsule of radio wave blocking material, for example aluminium. Used to protect the RFID-chip in biometric passports from being read at other times than when reading is expected.

'**Brute force**': A trial-and-error approach to break a cryptographic key or code.

'**Man-in-the-middle**': An attack where the attacker places him-/herself invisibly between communicating entities relaying the communication, trying to steal keys, codes and/or information.

'Digital Signature': "A digital signature is a construct that authenticates both the origin and contents of a message in a manner that is provable to a disinterested third party"[4]. In this context, and a more easily understandable language, this means that a digital signature is a way of guaranteeing that the data is not tampered with and that the (correct) government has issued it. However, the digital signature does not guarantee that the ePassport, or more precisely the RFID chip inside, is genuine. Digital signatures are made possible by a PKI (see abbreviations).

'Cipher': A systemized way to change information into something only the people with the correct deciphering key can understand. This method of sharing secrets has probably been used in some form as long as people have communicated, at first using looks, body language, agreed-upon terms or other secret 'keys'. When the written language was invented, the idea of replacing different symbols with others using some kind of mathematical or logical system was born. In modern cryptography, streams or fixed-size blocks of digital information are encrypted and decrypted using highly advanced cipher systems. For simplicity, we range the security level of a cipher system as 'broken', 'broken but secure enough for insensitive information', 'computationally infeasible to break' (meaning the computer calculation power needed to break the cipher is – not yet – available) or 'not (yet) broken'. Broken also means susceptible to cryptanalytic attacks.

1.1.6 Abbreviations

RFID (chip): Radio Frequency IDentifier (chip) is a family of small chips that are capable of permanently and/or temporarily store information and duplex communication with a reader using radio waves. For more information see chapter 1.2.1.

ICAO: the International Civil Aviation Organization, the issuer of the biometric passport standard currently being applied. The ISO 7501-1:2005 is a short form of the ICAO standard.

ACLU: American Civil Liberties Union. The US' "*guardian of liberty*", the ACLU works in courts, legislatures and communities "*to defend and preserve the individual rights and liberties guaranteed to every person in this country by the Constitution and laws of the United States*" [5].

ISO: International Organization for Standardization.

US-VISIT: United States Visitor and Immigrant Status Indicator Technology program [6].

MRTD: Machine-Readable Travel Documents, an abbreviation used by the ICAO, meaning machine-readable passports, visas and official travel documents. The machine readable

information is at present either contained in a machine-readable code or a Contactless Integrated Circuit (IC), i.e. an RFID chip.

MRP: Machine-Readable Passport. See also the definition of MRTDs above, as a MRP is an example of an MRTD. MRP is the foundation for the new ePassport.

VWP: The Visa Waiver Program, of which Norway participates, enables most citizens of the 27 member countries to travel to the US for 90 days or less without having to obtain a visa [2]. These countries must from October 2006 provide their citizens with biometric passports to continue the program. The VWP is a part of the US-VISIT program.

NSM: "Nasjonal Sikkerhets Myndighet", the Norwegian National Security Authority is "A preemptive security service, which strives to protect sensitive information and objects from security threatening actions" [7].

BAC: Basic Access Control, a means to ensure that communicating entities are who they claim to be. More on this in section two of the literature review chapter.

FAR: False Acceptance Rate, a standard term used in biometrics identification systems, meaning the probability of a person being falsely identified as another person than him- or herself.

FRR: False Rejection Rate, a standard term used in biometrics identification context, meaning the probability of a person not being identified as him- or herself.

PKI: Public Key Infrastructure is a system using public keys to verify that data is indeed from the entity it is supposed to be, and that the data has not been changed since it was issued. The data is encrypted using a secret, private key, and can only be decrypted using the corresponding public key.

MRZ: The Machine-Readable Zone is the two lines on the bottom of the MRP data page. These lines can be read by machine and contains some of the same information as is written on the rest of the data page.

1.1.7 Assumptions

The main assumption in this study is that the information needed is available to us. The ICAO standard is publicly available, but costs approximately $ 250. However, this document contains three more or less separate parts, only one of which is directly linked to E-passports, named "Part 1 – Machine Readable Passports". Other information, especially concerning governments' implementations of the passports, might be more difficult to obtain. Most, if not all, of the information concerning ePassports is only available on the Internet, which means we must carefully select reliable sources.

As the US is the initiator of the electronic passport policy, we believe it is likely that this country's development may be more advanced and more thought through at present than most others. The first part of this assumption is supported by the article we use for our literature review [8, p 10]. We also think other governments may look to the US implementation of the ICAO standard, so their experiences could be the basis for other countries. Therefore we believe the US implementation is of such importance it would be smart to include it in our

work with sub problem 3 ("View the implementation of the ICAO standard by chosen governments in search for differences").

We also assume that, in the case of the electronic passports, many aspects of privacy and security intertwine. The electronic, and now biometric, passports are being implemented to improve the security of immigration worldwide [9]. The uses of digital data and automated procedures for biometric recognition of individuals are believed to increase security. The security of the passports themselves may have been improved, but there are other considerations. Several experts and organizations have voiced serious concerns about the privacy of biometric passport owners. Privacy concerns are not opposite of security concerns, but the two may interfere with each other, and privacy is often best protected using security mechanisms. Therefore, the privacy of passport owners is a major security concern, and will be treated as equally important in this paper.

The last assumption is that we will actually be allowed to complete this project. The Head of Studies ICT, Stein Bergsmark, brought to our attention that we might need to make the Norwegian National Security Authority (the NSM) aware that we plan to perform a project concerning electronic passports. This, albeit doubtfully, might be deemed a threat to national security, and we should take this into account.

To ensure the legality of our project, we sent a mail to the NSM explaining our project and requesting their approval if needed. The mail is situated in Annex A and was authored in cooperation with another group also producing a master thesis on ePassports. The NSM, however, did not respond to our request, so we assumed they did not have any objections.

1.1.8 Initial Concerns

We have, naturally, some initial concerns in this project. These are listed below.

Several versions of the new passports have been presented, resulting in a general confusion over which name suits what version. Specifically, a passport with a machine-readable code on the data page is simply called a machine-readable passport; a passport with an incorporated datachip is known as an electronic passport; and if the chip contains biometric data about the owner, the passport is called biometric. For simplicity, the ICAO TAG/MRTD uses the term ePassport for biometric passports. It is our impression that many do not know of this distinction, and therefore, erroneously, add to the confusion. In this paper we will adhere to the TAG/MRTD terminology and use 'ePassport' to describe the electronic, biometric MRP.

The group responsible for developing the ICAO standard, the TAG /MRTD, consists of experts from 13 (Australia, Canada, Czech Republic, France, Germany, India, Japan, New Zealand, Netherlands, Russian Federation, Sweden, United Kingdom and United States) of ICAO's 189 member states.

"*Delegations to the TAG/MRTD are normally composed of government experts dealing with travel control issues, which might include the passport authority, immigration authority, customs authority, and/or national police authorities.*

Observers are also invited to attend TAG/MRTD meetings. Observers can represent either States or non-governmental bodies such as the Airports Council International (ACI), the International Air Transport Association (IATA), the International Criminal Police

Organization (INTERPOL) and the International Organization for Standardization (ISO)."
The experts' perspective is travel control. We wonder, are they capable to see all aspects?

Our area of (some) expertise is Information- and Communications Technology (ICT). This area is only one part of the big picture, and should be regarded as such. To complete this paper satisfactorily, we also need to consider other aspects, especially privacy.

1.1.9 Importance of our study

The use of RFID chips in biometrical passports raises great concern in certain areas, especially those of security and privacy. In recent years, Gillette, Wal-Mart and other organizations have received much negative attention regarding their use of RFID chips to improve supply chain management and other tasks. These chips have made it possible to track and make statistics on the movement of consumers, breaking baseline privacy requirements of the civil population. The concern is that privacy and security may not be satisfactorily considered in the new passports.

In addition, biometrics, although very intriguing, are still a relatively new way of computer-based identifying of individuals. It is argued that software for biometrical identification is still quite inferior to humans [10]. This raises concern that it may be easier to spoof an automatic identification system than the old, manual one.

Finally, the ICAO standard is only a guideline, and individual governments stand relatively free to implement whatever parts they wish, except the baseline standard, which, for compatibility reasons, must be implemented. Different types of implementations will necessarily have different security and privacy levels, which may in itself cause problems. In addition, three types of biometrics may be implemented, namely a photo of the passport's owner, his/her fingerprint, and his/her iris scan. These are ranged increasingly by their rate of secure identification, but the required one, facial recognition, is the least secure one. Why choose this one when the other two are far superior regarding positive identification?

1.2 Theory and Literature

This chapter starts with a presentation of the development of requirements for the US biometric passports over the year 2005. The year has been filled with public and organizational concern about the solutions for privacy and security in the new passports, followed by new requirements by the US state department. The second section of this chapter reviews the article "Security and Privacy issues in E-Passports" written by Dr. Ari Juels (at RSA Laboratories), David Molnar and David Wagner (both at the University of Colombia, Berkeley).

1.2.1 Overview of 2005 and the issues of biometric passports

As the United States of America publicly announced their plans about implementing biometric passports, there were almost immediate reactions from privacy organizations such as the American Civil Liberties Union (ACLU) [5] and Privacilla [11], security experts [12] and civilians [13] and [14, p 61553]. Their concerns included the "big brother sees you"-concept, and the security shortcomings of RFID chips contributing to the threat to privacy. We will concentrate on the ACLU statement, as it outlines the most central concerns of all these.

The ACLU initially protested to the use of RFID chips, due to the security and privacy shortcomings of the RFID chips the government planned to implement. In April 2005, the ACLU sent a letter to the US State Department, expressing concerns, especially regarding the RFID technology [5b]. The reading distance of RFID chips in general, up to 30 feet (more than 9 metres), was especially addressed as a threat. At this time, the US department had not announced what RFID standard would be used.

As the US chose not to encrypt the data on the chip, skimming, or unauthorized reading of the data on the RFID chip was made possible. This is more of a privacy attack than a security attack, but governments, who are responsible for protecting their citizens' right to privacy, must also address privacy concerns. The ACLU points out that the ICAO standard calls for a type of RFID chips that cannot be read at long distances.

The US government's reasoning for skipping encryption was that the digital information is the same as the printed information on the passport. The ACLU disagrees, and points out the individual's right to choose who will read the passport information, enabling them to protect themselves in some manner against unauthorized access to their personal information.

The ACLU especially notes that unencrypted information would make it quite easy to remotely decide the nationality or other traits of a passport owner. This would make anyone able to detect and track individuals of given nationalities, for example providing terrorists with an easy way to attack citizens of certain nationalities. It is not difficult to find other, either dangerous or simply annoying, reasons for knowing the passport owner's nationality, gender, age, even title, which is an optional field. As an example, many businesses would probably like to know these things about their foreign customers, to tailor their behaviour towards them. Identity theft is also mentioned as a possible result of skimming, also leading to passport forgery and fraud.

Another means of the government was to use an anti-skimming material on the front and spine of the passport, a so-called 'Faraday Cage'. This will protect the data while the passport is closed, but as soon as the passport is opened, there will be no protection of the communication between the RFID chip and the reader. Thus, listening the communication, or

eavesdropping, is possible. The government argued this would not be a problem, as eavesdropping equipment is large and difficult to place near ports of entry at airports or other borders stations. The ACLU argues that as time passes, the technology normally gets smaller, more powerful (and cheaper), and that eavesdropping can be successful at larger distances than normal communication. In addition, passports are not only used at border points of entry. Several hotels and cruise ships use passports to verify identity upon reservation. These environments may not be as well protected as airports or border stations. We will explain more about eavesdropping in the "Privacy and Security in E-passports" section of this chapter.

This comment was, as previously mentioned, sent on 4 April 2005. At present, the concerns discussed in the letter have been more or less eliminated. This doesn't make the document useless to our project, as it shows the initial weaknesses regarding privacy and security of the US biometric passports, and the public and organizational protests. The document sheds light on the need to address privacy and security issues, as many governments tend to choose the easiest and cheapest solutions, and it is difficult to take all aspects into consideration.

Several adjustments had to be made to the US biometric passports. On 9 August 2005, the government presented new passport requirements, stating: "*The new passport will combine facial recognition and contactless chip technology. The chip, which will be embedded in the cover of the passport, will hold exactly the same information that is printed in the passport: name, date of birth, gender, place of birth, dates of passport issuance and expiration, passport number, and photo image of the bearer. A digital signature will protect the stored data from alteration and mitigate the threat of photo substitution.*

To address concerns that the chips may be susceptible to unauthorized reading (skimming in the industry parlance), the Department will incorporate anti-skimming technology in the front cover. The Department is also seriously considering incorporating basic access control (BAC) technology in the new passport. BAC prevents the chip from being accessed until the passport is opened and its machine-readable zone on the data page is read electronically. The anti-skimming feature and BAC, when taken together, will prevent unauthorized reading of the Electronic Passport." [15]

In this statement, many security issues directly important to the US government was improved. However, no encryption of the data was considered. Neither was the question whether the chip should be passive or active addressed, nor was the use of Basic Access Control determined. It would only be seriously considered. This solution was deemed unsatisfactory from a privacy perspective, as none of the concerns of the public were addressed. A new ruling had to be made. The final rule was made public on 25 October 2005, stating: "*Passports must be globally interoperable--that is, they must function the same way at every nation's border when they are presented. To that end, the International Civil Aviation Organization (ICAO) has developed international specifications for electronic passports that will ensure their security and global interoperability. These specifications prescribe use of contactless smartcard chips and the format for data carried on the chips. They also specify the use of a form of Public Key Infrastructure (PKI) that will permit digital signatures to protect the data from tampering. The United States (U.S.) will follow these international specifications to ensure its electronic passport is globally interoperable (…)*

The ICAO specification for use of contactless chip technology requires a minimum capacity of 32 kilobytes (KB). The U.S. has decided to use a 64KB chip to permit adequate storage room

in case additional data, or biometric indicators such as fingerprints or iris scans, are included in the future. Before modifying the definition of ``electronic passport'' to add a new or additional biometric identifier other than a digitized photograph, we will seek public comment through a new rule making process.

The contactless smart chip that is being used in the electronic passport is a ``passive chip'' that derives its power from the reader that communicates with it. It cannot broadcast personal information because it does not have its own source of power. Readers that are on the open market, designed to read Type A or Type B contactless chips complying with International Standards Organization (ISO) 14443 and ISO 7816 specifications, will be able to communicate with the chip. This is necessary to permit nations to procure readers from a variety of vendors, facilitate global interoperability and ensure that the electronic passports are readable at all ports of entry.

The proximity chip technology utilized in the electronic passport is designed to be read with chip readers at ports of entry only when the document is placed within inches of such readers. It uses RFID technology. The ISO 14443 RFID specification permits chips to be read when the electronic passport is placed within approximately ten centimeters of the reader. The reader provides the power to the chip and then an electronic communication between the chip and reader occurs via a transmission of radio waves. The technology is not the same as the vicinity chip RFID technology used for inventory tracking of items from distances at retail stores and warehouses. It will not permit ``tracking'' of individuals. It will only permit governmental authorities to know that an individual has arrived at a port of entry--which governmental authorities already know from presentation of non-electronic passports--with greater assurance that the person who presents the passport is the legitimate holder of the passport(…)

Finally, the chip will contain coding to prevent any digital data from being altered or removed as well as the chip's unique ID number. This coding will be in the form of a high strength digital signature. The contents of the data page of the traditional passport have been established by international usage and by ICAO. The chip will not contain home addresses, social security numbers, or other information that might facilitate identity theft." [14].

In summary, this rule states that the technology used for data storage and contactless communication is RFID, more specifically, RFID chips conforming to the ISO 14443 standard mentioned earlier in this proposal. This means the chips will be passive and operate at 13.56 MHz. The intended read range is only about 10 cm at the present time. Basic Access Control will in fact be used to protect the data on the chip, but no encryption of the data will be done. The biometric will be re-evaluated at a later stage, meaning the US may be recognizing the inadequacies of facial recognition.

Looking back at the privacy concerns of ACLU and others earlier this year, this is definitely a step in the right direction. As we will see in the next section, it is, however, not enough to completely secure the information.

1.2.2 Security and Privacy issues in E-Passports [8]

This article was published in September 2005, and is therefore reasonably recent in the field of E-passport issues. The ACLU has already addressed some of the issues listed in the article, and these we may review in less detail than new ones. The article starts by summing up 6

main threats to privacy and security. These are based on both the RFID technology and the biometrics that will be used. The 6 threats are:

1 Clandestine Scanning, which can be accomplished from up to a few feet's distance. This is a bigger threat to passports that only implement the baseline ICAO standard, and do not include encryption, BAC and/or a Faraday Cage, which are optional.

2 Clandestine Tracking, made possible because each RFID chip must have an ID, which is emitted on protocol initiation, and used for link-layer collision avoidance. This ID, if unique for each passport, can be tracked. Even worse, information like nationality may be derived from it if the procedure for generating the ID makes this possible.

3 Skimming and Cloning, clones of passports is a major security issue, as people who look alike could possibly use the same passport, even without changing the digital photograph.

4 Eavesdropping, this is more problematic than scanning, as it is completely passive and therefore impossible to detect unless the actual device is discovered. It can also be achieved over greater distances than ordinary reading, especially if the eavesdropper has error-correction procedures. Eavesdropping is, as the name indicates, listening to (and recording) the communication between RFID chip and reader. This way the information on the chip can be obtained without directly accessing it. It may be argued that it will be difficult to place eavesdropping equipment at ports of entry, but this is likely not to be the only place where electronic passports will be used. Hotels and cruise ships already use passports for confirming identity, and areas like e-commerce will also probably make use of the new passports.

5 Biometric Data-Leakage, the need to keep biometric data secret is more and more important, as the process of authenticating the passports and their owners will be increasingly automated, and have less human oversight.

6 Cryptographic Weaknesses, simply encrypting the data and/or communication of the RFID chip using any given encryption scheme is not enough. If the encryption or key(s) used do not withstand probable attacks, scanning the chip or eavesdropping on the communication will not be difficult. A false sense of security is in our opinion worse than knowing that you are vulnerable to attack.

The first three points have been discussed in more or less detail in the media, while the latter three are more technically oriented, and might be better discussed in a more professional forum. The article provides an overview of these, with a review of parts of the ICAO standard's chosen technologies, algorithms and procedures relating to security and privacy.

The final rule of the US state department says that social security number, home address and "other information that facilitate identity theft" will not be included on the chip, the article, however, argues that the photograph, name and birth date, which will all be included, is a head start to successfully steal someone's identity.

Next, the article looks at the biometric threats, and, like the ACLU, concludes (against the US state department) that the increased automation and decreased manual oversight calls for biometric secrecy. In addition, the (optional) fingerprint image may be important for an individual to keep secret, as new technologies allow us to unlock our home, home computer or other items using fingerprints. This is also true for iris scans. The digital photograph of the

passport owner may not have these issues, but because the photo has such a good quality (lighting, perspective, background), it could actually spoof some face-recognition systems.

The ICAO standard includes two optional, and one mandatory cryptographic feature for the passports. The mandatory one is *Passive Authentication*, meaning the information on the chip will be digitally signed by the issuing nation. The permitted signature algorithms include *RSA*, *DSA* and *ECDSA*. The fact that the signature only ensures that the data, not the chip (passport), is authentic is emphasized.

The first optional feature is *Basic Access Control (BAC)* and *Secure Messaging*. The first part, BAC, initiates the other. A pair of cryptographic keys (K_{ENC}, K_{MAC}) are stored on the RFID chip. When an attempt to read the information on the chip is detected, it starts a challenge-response protocol that proves knowledge of K_{ENC}, K_{MAC}, and a session key, which is used for Secure Messaging, is derived. The algorithm for this challenge-response protocol is outlined in [8, p 8].

K_{ENC}, K_{MAC} must be possible to derive from the optically readable information on the passport, specifically the passport number, the date of birth of the bearer, the date of expiration of the passport and three check digits, one for each of the preceding values. This, according to the article's authors, is too small at present. The ICAO PKI Technical Report says that the entropy is at most 56 bits, and that some of these bits may be guessable. The authors, after some logical reasoning over what the values of the information may be, claim that the entropy of the US passport may be even smaller, about 52 bits. Some other countries are even worse. The Dutch passport is reported to only have about 35 bits of entropy, which a laptop computer can break by brute force in a few hours.

Another concern is that a single fixed key is used for the entire lifespan of a passport, meaning that there is no way to revoke access to the chip. The question is whether a person wishes any nation he or she has visited to have complete access to his or her personal data.

The other optional feature, which the ICAO specification urges use of, is *Active Authentication.* This is an anti-cloning feature, meaning it is especially interesting in a governmental point of view. It relies on public-key cryptography, making the RFID chip prove its possession of a private key. The corresponding public key is stored with the signed data on the passport. In this procedure, the passport reader initiates a challenge-response protocol, in which the chip on the passport must respond correctly, or it fails the test. The algorithm for this protocol is outlined in [8, p 9].

The public key used in Active Authentication must, like the BAC keys, be tied to the passport, or more precisely, to the specific passport and the biometric data on it. If not, a man-in-the middle attack is possible. The authors also emphasize the importance that the private key never leaves the passport (if it did, anyone could steal it and use it, meaning it would no longer be private). This is not explicitly stated in the ICAO standard. The authors also express some concern about the Active Authentication keys' interaction with the BAC keys. In some cases, the keys might compromise each other.

Three of the US government's reasons for not including the cryptographic features in the passports are then listed and discussed. These are: (1) The data stored on the chip are identical to those printed in the passport; (2) Encrypted data would slow entry processing time; and (3) Encryption would impose more difficult technical coordination requirements among nations

implementing the e-passport system. Also, the Faraday Cage is expected to be sufficient protection of the information.

The first reason has already been deemed flawed, both by this article and the ACLU comment. The second is a bit more difficult to discard immediately, but as both Active Authentication and BAC needs an optical scan of the passport (to obtain the keys), implementing one of them makes implementing the other in addition close to free. Some time will be spent performing the procedures, but this is not even mentioned in the article, so we expect it to be insignificant. It is probably in the size of seconds, maybe even less. The third reason is not even valid, as almost no coordination is necessary between the nations who implement the system. All information needed to derive keys is present on the passport, so the only coordination would be tied to which algorithms to use. This article does not find Faraday Cages to be sufficient protection of private information, because it provides no protection against eavesdropping, and electronic passports will probably be used in other areas than border security. The security at these locations cannot be standardized or enforced. Faraday Cages has therefore been deprecated in favor of BAC. It is, however, a good first line of defense.

In order to strengthen the electronic passports, the article suggests making the keys for BAC larger. More specifically, 128 bits. Another means to make the passports more secure is to make the collision avoidance ID mentioned earlier dynamic.

Finally, some future issues of E-passports are mentioned. One of these is the wish to include digital visas and “other endorsements”. Since two RFID chips close to each other could interfere with each other’s communication, all information would probably have to be placed on the same chip. This creates the need for writing new data on the chip after issuance, and the article suggests an area of append-only memory on the chip. This information might not be what the passport owner wants in his or her passport, as some countries denies entry to individuals who have visited certain other countries in the recent history.

So-called function creep, meaning that the new passports could be used in different contexts than the intended one, causes another future issue. This will probably create problems we cannot even imagine at the present time. Data protection features can be undermined, as the bearer’s data will be spread over divergent systems. Users may also call for greater convenience as time passes. A widely accepted theory is that security measures and convenience do not mix well, so this may also cause problems.

In our opinion, this article sums up most of the privacy and security concerns we have come across in our literature search. It certainly addresses some of the issues we intend to study in our project. Dr. Ari Juels is currently either the author or co-author of at least five other recent scientific research articles on RFID and privacy/security, so his work in this area is extensive.

1.3 The Gathering and Interpretation of Data

This project is primarily a literature study, and contains both quantitative and qualitative properties. Literature studies are often qualitative in nature, but in order to arrive at our final conclusion, we probably also need to quantitatively analyze the ICAO standard and the security and privacy measures therein. A purely quantitative research method may however overlook important aspects. Governments consist of human beings, as does the general population. These groups decide how E-passports will be implemented and used, and quantitative methods may miss some of the nuances of human actions. It is important to grasp the big picture, and therefore a qualitative approach is just as necessary. All professional research and governmental publications must be assessed both in a qualitative and quantitative manner.

To solve our first and second sub problems ("Determine the quality of the ICAO standard, and evaluate the technical and practical solutions presented in the document" and "Present and evaluate possible solutions to weaknesses we might find in the ICAO standard"), we need to study the ICAO standard. The first section of our project includes critical analysis of the quality of different technologies.

The document is an essential part of both sub problem 1 and 2, and should probably be studied and analyzed quantitatively for the second sub problem, which is directly dependant on the first. It consists of solutions to what we have previously discovered.

To solve our third sub problem ("View the implementation of the ICAO standard by chosen governments in search for differences"), we will need to search governmental statements focusing on what type of ePassport methods they will implement. It will probably be a good idea to make an overview of what features of the ICAO standard is to be implemented by which nations, and try to list as many of the nations possible in it. We have already seen a table doing just this in the article we have reviewed in the second part of chapter 3 [8, p 9]. This table is presented in Figure1.

Country	RFID Type	Deployment	Security	Biometric
Malaysia Gen1	non-standard	1998	Passive Authentication + Unknown	Fingerprint
Malaysia Gen2	14443	2003	Passive Authentication + Unknown	Fingerprint
Belgium	14443	2004	Unknown	Photo
U.S.	14443	2005	Passive, Active Authentication	Photo
Australia	14443	2005	Unknown	Photo
Netherlands	14443	2005	Passsive, Active Authentication, BAC	Photo
Germany	14443	2005	Passsive, Active Authentication, BAC	Photo

Figure 3. Current and near-future e-passport deployments. The Belgium, U.S., Australia, and Netherlands deployments follow the ICAO standard, while Malaysia's deployment predates the standard. The chart shows the type of RFID technology, estimated time of first deployment, security features employed, and type of biometric used. Here "BAC" stands for Basic Access Control. "Unknown" indicates a lack of reliable public information.

Figure 1 Table from "Security and Privacy in E-Passports"

The "Unknown" status of the 'Security' column for Australia and Belgium we have recently revised [16] and [17]. Both countries' security methods include Passive and Active Authentication and BAC. Belgium also uses Diffie-Hellman based Extended Access Control, which prevents unauthorized access to or skimming of biometric data [18].

The list enables us to determine what different governments emphasize in terms of security and privacy. Knowing what is important to governments in general makes our conclusion easier to reach, as the knowledge provides us with an initial measure of what is deemed 'secure enough'.

The table we have copied may act as a model for comparison for the different information we obtain. We believe it could provide a good starting point for our analysis, but we will also need to use some qualitative research methods to provide a good overview of the complete e-passport system in an international perspective. It is important for governments to see the "big picture".

In our dealings with sub problem 3, we encounter our first really qualitative method. We have chosen to go in-depth on two or three (The US, Norwegian and if information on the latter is scarce, or other countries' implementation presents particularly interesting scenarios, other will be chosen from table in Figure 1) of the passport implementations, so-called case studies. The results of this part must however be presented more quantitatively to be useful to our fourth and final sub problem ("Sum our findings, and determine as best we can whether the new ePassports really are secure enough. Based on this, we can also try to recommend a minimum implementation that eliminates the most critical problems, if any.").

The fourth sub problem may prove to be the most difficult one. It is the summary of the other three, but also an attempt to take a step in the direction of more secure ePassports. The solution of this problem will only by reached by analyzing our results from other parts of the project.

Some information has already been obtained, but we believe much of the first weeks will be spent in search of relevant information. This will be: Government publications, professional research in most areas of e-passports, professional research of the methods implemented by the ICAO standard (or other, non-standard methods), and other relevant, professional literature. This information is available both at the Internet, at the school library or by contacting the correct department. Some information may be confidential, or cost money, but if the availability of the information on the US passport is a good indicator, much will be possible to obtain.

When the information has been secured, it will be necessary to write a qualitative review of it, focusing on and quantifying the information relevant for our sub problems. If we are to discover whether the different implementations create new security problems, we need to study other research.

2 RFID

RFID (Radio Frequency IDentification) is traditionally a system for tracking products. The system has its root in the Second World War, were it was used to identify friendly aircrafts. The technology that was in use during the Second World War was named Identify Friend or Foe (IFF). After the war this technology was developed for new applications and used to track military equipment and personnel, RFID was born. In the late 1970s companies made an effort to commercialize RFID tracking technology, and during the last couple of decades RFID has become a well-known method. [19].

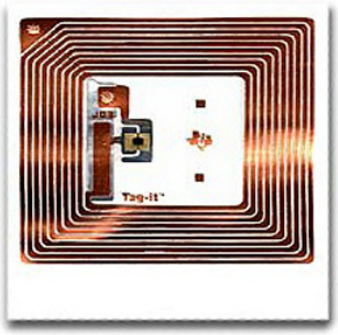

Figure 2 RFID tag

RFID is now a technology for automatic identification of objects, animals and people. RFID is a subset in the automatic identification (Auto-ID) class [20]. Auto-ID is a term for all automatic identification systems for commercial use, which includes barcodes, smart cards and optical recognition systems. RFID is the most important, discussed and well-known system of all automatic identification systems.

An RFID chip, which may also be called an RFID tag, is a small microchip designed for wireless data transmission. This microchip is generally attached to an antenna in a small package. In ePassports this package is a part of the passport cover in the passport book [21]. There are two types of RFID tags, active and passive [19]. Active RFID tags have both an on-tag power source and an active transmitter. Since they are connected to their own battery they have superior performance. Actually the read-range can be several kilometers. The passive RFID tag was invented in 1969 and patented in 1973 [20]. Passive tags have no power source and on-tag transmitter. That gives them a range of less than 10-meters, and also makes them sensitive to regulatory and environmental constraints.

To make an RFID system work, every system consists of two integral parts: a tag and a reader. Readers interrogate RFID tags. When the RFID tag is passive the RFID reader transmits an energy field that powers the microchip in the tag, enabling it to transmit or store data. Active tags, however, may periodically transmit a signal so that multiple readers may capture data.

During the last decays there has been constant development of new applications of RFID. Some of the most common uses for this technology are the following:

- *Proximity cards.* Contactless cards used for building access.
- *Automated toll-payment transponders.* Small plaques positioned on the inside of the windshield.
- *Theft-deterrent in ignition keys of many automobiles.*

- *Payment tokens.* Examples are SpeedPass, American Express ExpressPay and Mastercard PayPass.
- *Pet control.* Identification of pets are often done by an RFID chip.

In the future we will probably see more use of RFID. Here are some of the possibilities:

- *Smart appliances.* Like a refrigerator that warn you when you are low on some food or something has expired, or washing machines that select the wash cycles automatically.
- *Shopping.* For example the system can automatically tally items, compute the total cost and charge the consumers' RFID-enabled payment devices.
- *Interactive objects.* A consumer can for example scan a movie poster to display show times on his/her mobile phone.
- *Medication compliance.* An RFID-enabled medicine cabinet could help verify that medications are taken in a timely fashion.

In ePassports RFID is used for two reasons; more or less automatic scanning of the passport and the possibility to add biometric features in the passport. The specifics of RFID chips used in biometric passports are addressed in the ISO 10536, 14443, 15693, 7816 and 10373 standards [22]. The RFID chips used in the biometric passports are compliant with the ISO 14443 standard, which specifies a radio frequency of 13.56 MHz; an intended read range of approximately 10 cm; and that the RFID chip may not contain an internal power source, which means it must derive power from the reader's signal. This makes the biometric passport RFID chip *passive*, meaning it does not communicate at all until it is asked to.

Every RFID system could be in danger of being attacked in some way or another. There are several threats for an RFID system. These can be both security and privacy threats. Passports include most of the personal information; therefore privacy is an important issue when it comes to ePassports. The STRIDE threat model is a model that can be used for analyzing most information systems, and this model is also valid for RFID systems [23]. STRIDE is an acronym for six threat categories. These are the following:

1. **S**poofing identity
2. **T**ampering with data
3. **R**epudiation
4. **I**nformation disclosure
5. **D**enial-of-service
6. **E**levation of privilege

A relatively new threat for RFID is the ability to create viruses that can attack the RFID tag, or systems communicating with the tag.

3 Biometrics

"*Biometrics is the automated measurement of biological or behavioural features that identify a person*" [4, p. 328]; or "*Biometrics are the automated means of recognising a living person through the measurement of distinguishing physical or behavioural traits.*" [24, p. 8].

In other words, using biometrics means collecting and using information about personal characteristics that uniquely identifies an individual. The different characteristics are usually divided into two categories, behavioural and physical. Techniques used for identification using behavioural characteristics include keystrokes dynamics, voice recognition and signature dynamics, while techniques using physical characteristics may be iris recognition, retina recognition, vein pattern recognition, face recognition, recognition of hand or finger geometry and fingerprint recognition [25].

All humans use biometrics, in particular facial features, voice characteristics and bodily characteristics, among others, to identify people they know. During the last century, techniques for using biometrics to legally, or officially, identify individuals have been developed, especially using fingerprints, dental features and DNA. Popular Science Fiction- and Action movies have for decades experimented with biometrics as means of secure identification (and often grotesque ways to beat this type of system), and been one of the motive powers in the development of biometrics techniques.

The different types of unique features of the individual call for different techniques for sampling and treatment of biometrics data, and one type of biometrics can be treated in several different ways. For example, fingerprints can be treated as a complete picture, which is visually compared to another picture to locate similarities.

Another way of treating fingerprints (or other biometric identifiers) is by computationally locating small details of interest in the pattern. Such characteristics are called minutiae, and may be bifurcations, ridge endings, deltas and the core [26]. The minutiae (their type and location) can then be given numerical values, which are sent through some algorithm to create a checksum, or a template representing the unique characteristics of this particular fingerprint. The different types of minutiae are presented in Figure 3 below, which we have copied from Carlsen's presentation.

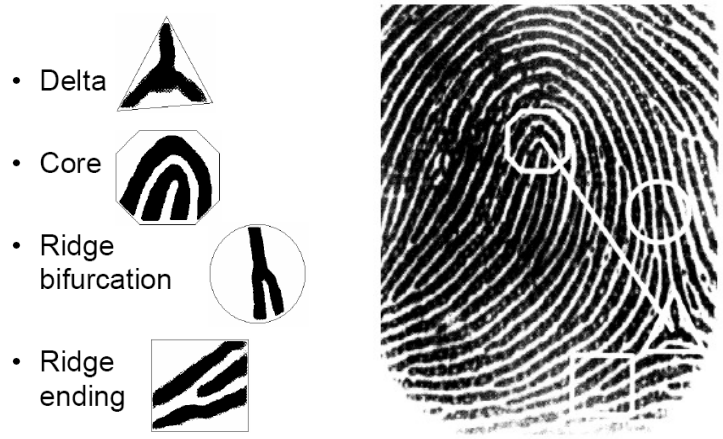

Figure 3 The minutiae of a fingerprint

Whenever the fingerprint pattern of the individual needs to be checked, the minutiae from his or her fingerprint will be sent through the same algorithm as the original sample. The new sample is compared to the stored template, and if the two have a satisfactory degree of similarity, the identity is confirmed.

The first method is based on the standard method we humans use to recognise each other, and is best suited for human comparison. The second is a more mathematical approach, and is suited for automated identification. Computer systems may use this method much more effectively than humans. In general, computer assisted methods of identification based on biometrics use discrete values mathematically representing the biometric characteristics to create templates for a given person's identity.

In the ePassport context, both methods may be applied. The facial photo is stored in a compressed version, and the biometric data of fingerprint is stored as a template. The RFID chip has very limited data storage capacity. The ICAO TAG/MRTD standard demands at least 32 KB storage capacity on the RFID chip [27], which, in theory, is enough to store 32 000 letters in basic ASCII-code (each letter is represented using seven bits, the eighth bit of each byte is used for error-checking functions), or, put differently, about five times the text of this chapter, which contains almost 6 300 letters. This is without file allocation data, which is necessary if you wish to access the data again once it has been stored.

This may sound like a lot of data, but pictures require much more storage space than characters. Specifically, the digital picture specified by the ICAO standard will without compression require almost 650 KB! Using JPEG and JPEG2000 compression the storage requirement might be reduced to only 12 KB, but more serious compression would, according to the ICAO, cause too unreliable facial recognition. The ICAO states that 15 – 20 KB will be the optimum storage size [24].

Mathematical representation of biometric data is not an exact science, only an approximation. [26]. The ICAO encourages all member states to research sampling- and recognition algorithms and individually decide on how accurate matching must be [24].

We will make a short presentation of the automated procedure for fingerprint recognition. A fingerprint generally contains about 100 minutiae, but the area scanned by sensors contains from 30 to 40. In European Courts, a fingerprint match is valid if at least 12 matching minutiae are found [25].

To extract a minutiae template from a fingerprint, several picture processing techniques need to be applied [26]. These include:

- Image capturing (in greyscale)
- Contrast enhancement / normalisation (spreading pixel values evenly along the black/white scale)
- Contextual filtering (extrapolation of ridges, separation of nearby ridges and increasing contrast between ridges)
- Binarisation (assignment of binary values to pixels, global median, local median)
- Quality markup (removing surrounding "landscape" and bad image areas), and
- Minutiae detection.

The type and coordinates of the detected minutiae are stored as a template in the database containing other relevant data belonging to the owner. Whenever a new sample is taken, this

is compared to the stored template. According to manufacturers of fingerprint scanners, if the requirement is 8 matching minutiae, there is a false acceptance rate (FAR) of about 1 in a million. The FAR of course increases rapidly by requiring more matching minutiae.

The procedure for face recognition is somewhat different in nature, and is based on human techniques for recognition, using a larger scale. Some of the unique identifiers in a face include the geometry of the face as a whole, distances and directional vectors between for example nose and chin, chin and cheekbones, the eyes and depth of the eye sockets [28]. The distance-procedure may also be used on the palm of the hand, or sole of the foot. The algorithms used for face recognition are constantly evolving and improving, as there is a considerable research effort being made in this area.

4 The ICAO Standard for ePassports

The internationally applied standard for ePassports has been developed by the ICAO 'Technical Advisory Group on Machine Readable Travel Documents', or the TAG/MRTD for short [1]. At present, this group consists of experts from 13 ICAO member countries, namely Australia, Canada, the Czech Republic, France, Germany, India, Japan, New Zealand, the Netherlands, the Russian Federation, Sweden, the United Kingdom and the United States.

In addition to regular members, observers, i.e. representatives from various countries and organizations, can also attend meetings of the TAG/MRTD. As examples of organizations, the ICAO MRTD website mentions the Airport Council International (ACI), the International Air Transport Association (IATA), the International Criminal Police Organization (INTERPOL) and the International Organization for Standardization (ISO). Especially ISO has played and still plays an important role in the development process.

The ICAO standard for Machine Readable Passports is outlined in a document called "Doc 9303 Part 1 for Passports" [9]. Doc 9303 also consists of two other parts, namely "Part 2 for Visas" and "Part 3 for Official Travel Documents (cards)". The latest version of part 1 of this document was published in 2003. At that time, no guidelines for RFID chips or biometrics existed, so technical reports describing use of these technologies have been issued at a later time. The latest supplement to Doc 9303 was published December 2005. This supplement gives an overview of which technology will be issued in the next release of Doc 9303, scheduled to be released within 2006. In the next release of "Doc 9303 Part 1" ICAO will have guidelines for ePassports. The new version will come in two volumes, and volume two will contain the specifications for an enhanced MRP with biometric data encoded in a contactless integrated circuit (RFID) chip.

ICAO has also released a report called "Biometrics Deployment of Machine Readable Passports" [24]. This report includes the ICAO vision of biometric passport. The report is more an overview of other technical reports about the issue, than it is a technical overview itself. This report was issued in 2004, and technology and so forth have changed since that time. Some new thoughts are outlined in a fairly new report called "ICAO MRTD report" [31]. This report was released early 2006.

There are at least three kinds of biometric data that are allowed stored in the RFID chip, and be used for identification of the passport holder. These are; fingerprint, iris scan (or retina scan) and facial recognition. More information about these features can be found in chapter 3.

The ICAO standard provides some guidelines about how to secure the information stored at the RFID chip. A lot of this is presented below.

4.1 About the Ciphers Used in ePassport Security Measures

[4,29,30]

We recommend visiting Wikipedia online for more information about the mathematics involved in the ciphers. We have gathered most of the information in this section from this website. The basic algorithms for key generation are presented in Annex B, and are also gathered from Wikipedia.

In general, Digital Signatures can ensure two things: That information indeed originated where it claims (the issuer signs the information encrypting it with his or her private key and it can then only be decrypted using the corresponding public key), or that information is only read by the correct recipient (the information is encrypted using the recipient's public key, and can then only be decrypted by the one who possesses the corresponding private key. Digital Signatures are an integral part of ePassport Passive and Active Authentication, and algorithms that governments may use for Digital Signatures include: RSA, DSA and ECDSA.

The RSA algorithm is from 1977, and is still going strong. The name consists of the initials of the three scientists at MIT who described it. The RSA cipher is the first one known to be suitable for digital signatures and encryption. It is an exponentiation cipher, meaning that it uses repeated multiplication. It is regarded as secure, as long as sufficiently long keys are used. The RSA uses two keys, one public and one private.

The Digital Signatures Algorithm (DSA) is a US Federal Government standard for digital signatures. It was first proposed in 1991. DSA relies on the mathematical problem of solving the discrete logarithm problem.

The Elliptic Curve DSA, or ECDSA, is a variation on the DSA, using elliptic curve groups (an elliptic curve is an algebraic curve defined by an equation on the form $y^2 = x^3 + ax + b$). Using elliptic curves provides smaller key sizes for the same security level, while execution time and signature size are roughly or exactly the same, respectively, as for DSA.

RSA, DSA and ECDSA differ from one another in the mathematical techniques used for key generation, encryption and decryption and signature verification algorithms.

For encryption of the messages used for the BAC protocol and Secure Messaging, the ICAO requires the use of two-key Triple DES in CBC mode. DES, or the Data Encryption standard, is the oldest of our ciphers. It was selected as an official Federal Information Processing Standard (FIPS) for the US in 1976. It has been frequently used, despite some suspicion of a NSA backdoor. The key used is only 56 bits of length. Today, basic DES is considered too insecure for many purposes because of the short key, but is improved to "believed to be practically secure" using the cipher three times, so-called Triple DES, or TDES. TDES generally uses three keys and enciphers the chosen information three times (EEE). Thus, the effective key length is tripled to 168 bits.

The middle encryption may be replaced by decryption (EDE), for interoperability between TDES and DES. If the three keys were all equal, TDES with encryption-decryption-encryption would in fact be the same as single DES. In the passports, two keys TDES is used, meaning that two of the three keys, namely number one and three, are alike. This makes the effective key length 112 bits, but because the mode is susceptible to certain chosen plaintext and known plaintext attacks, the official designated number of key bits is only 80.

DES, and TDES, is disappearing from use, replaced by Advanced Encryption Standard (AES), which in essence is DES' successor. It is much faster and offers markedly higher security margins, i.e. a larger block size, potentially longer keys and (as of 2005) freedom from cryptanalytic attacks. However, the use of two-key TDES is still favoured by the electronic payments industry and in hardware implementations.

CBC mode, or Cipher Block Chaining, is a cipher technique used to prevent identical information to generate identical cipher texts. This may be used to break the cipher. CBC simply exclusive-ors any block with the preceding cipher text block before the block is encrypted. This method requires an initialization vector to be exclusive-or'ed with the initial plaintext block. The vector must be stored on the RFID chip along with the two keys and be treated as equally secret.

The ICAO has issued recommendation for minimum key sizes, taking into account the ten-year expected lifetime of the ePassports. The recommended key sizes are:

- RSA:
  - Country Signing CA Keys: modulus n 3072 bits
  - Document Signer Keys: modulus n 2048 bits
  - Active Authentication Keys: modulus n 1024 bits
- DSA:
  - Country Signing CA Keys: modulus p 3072 bits, modulus q 256 bits
  - Document Signer Keys: modulus p 2048 bits, modulus q 224 bits
  - Active Authentication Keys: modulus p 1024 bits, modulus q 160 bits
- ECDSA:
  - Country Signing CA Keys: base point order 256 bits
  - Document Signer Keys: base point order 224 bits
  - Active Authentication Keys: base point order 160 bits

5 National Implementation

Our main focus is on the Norwegian and United States' implementations of the ICAO standard. We list several reasons for this. First, the United States started work on their ePassports earlier than any other country (except Malaysia, but their passport does not follow the ICAO standard), so they have had several rounds with experts, the public and privacy organizations, especially the American Civil Liberties Union (ACLU). Second, the US' process of developing and issuing the passport has been highly open to the public, so we have been able to follow the discussion in retrospect. Our focus on the Norwegian implementation is based on the fact that as Norwegians we can get firsthand information from our government. Norway is also the third country in Europe to implement biometrics, and can in some degree be seen as pioneers in the context of ePassports. It is also easier for us to follow the development in Norway than in other countries since the press will cover every new aspect, we hope.

The ICAO standard gives a guideline for which features nations can implement. There are few rules of what features must be implemented, and that results in many differences that an inspector has to be aware of. These differences could be in what kind of information to implement, and it could be differences in appearance and security features. More information about this is available in chapter 8.

There are about 110 of the ICAO members that have issued Machine Readable Passports (MRP) and more than 40 countries are planning to upgrade to the biometrical enhanced version by the end of 2006 [31, p. 8]. All 189 ICAO members must issue only ICAO-standard MRPs within 1 April 2010, with or without biometrical enhancement. In Norway the MRP have been in use for some time now, at least since late 2004. Biometric passports with facial recognition have been issued in Norway since 3 October 2005, and from 2008/2009 they will also include fingerprints.

Norway was the third country in Europe to implement biometrics in the passport. Sweden started implementing biometrics 1 October 2005 [32], and at the same time they started to issue eID (electronic IDentification) [32b] as an alternative to the usual passport for use in the so-called Schengen countries (Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Switzerland and Spain). In other words, if the holders bring this identification card into these countries, they do not have to bring their passport. This identification card follows the ICAO standard as well. Both the ePassport and the identification card have a lifetime of five years in Sweden, while the ePassport have a lifetime of ten years in Norway. Denmark will start issuing ePassports from 1 August 2006 [33].

Belgium was the first country to issue ePassports in the world [34]. In fact, Belgium received the 2003 Interpol award for the best and most secure passport in the world. Belgium has for several years used a national database containing personal information of all citizens, more or less eliminating identity theft, which was a large problem in the past. The issuing of Belgian passports is based on the information in this database. The database could only become a success because of the severe Belgian privacy legislation. Citizens trust their government and have full access to their own information online. The security of the database is very strict, and all queries for information are properly logged. The logs are also available to citizens whose information has been queried.

Belgium also has some of the most serious security mechanisms available implemented in their ePassports. In addition to the commonly implemented Passive Authentication and Basic Access Control, Belgian ePassports also implement Active Authentication, Extended Access Control and an active anti-skimming feature, meaning information can only be accessed if the holder permits it [17].

The ICAO standard allows for a high level of freedom in individual governments' choice of security and privacy implementations. However, there are some areas where the ICAO chooses to recommend certain measures be taken. One of these is the effective lifetime of ePassports, and the ICAO provides several reasons for why five years should be the maximum lifetime [24, p. 47]. These are:

- Chip technology is changing at a rapid rate and a shorter validity period enables more rapid takeup on new technology
- Most Chip applications assume a chip/smartcard validity of 2-3 years – how such technology will perform over 5-10 years is yet to be tested in real world applications as the technology typically has not been deployed with consumers for that length of time
- Biometrics technology is changing at a rapid rate, so a shorter validity period enables re-enrolment using more sophisticated technology
- Most countries wish/need to turnover their passport booklet design every 5 years to keep ahead of counterfeiters
- Security printing techniques are undergoing continual improvement, so it is desirable to turnover passport booklets more quickly
- Security attacks on the data in the chip will become more sophisticated over time, so it is desirable to turnover passport booklets more quickly, enabling chip security protection mechanisms to be updated
- Performance of biometrics can tend to decline over time (eg compare 10 year old photographs vs 5 year old photographs)
- Turnover of passport applicants on a more regular basis allows rechecking of their bona-fides against new available databases eg online breeder document verification may have become available since the applicant originally applied
- Child applications typically already have 5 years validity so such a change would bring adult validity in line with child validity

Despite these recommendations, several governments, like the US and Norway, choose to keep the ten year validity. Others, like Sweden and Belgium have settled on a five-year lifetime.

6 Issuance

Any security system is only as good as its weakest link. What procedures exist to ensure that the individual receiving the passport is indeed who he or she claims to be?

The Norwegian system for issuing ePassports closely resembles the traditional issuing system. The applicant must present identification papers, like a birth certificate, driver's licence or similarly accurate documentation. In addition, he or she must provide a passport photo no more than 6 months old of him- or herself. At present, a visual comparison is made of the photo and the applicant. The information is sent to the Finnish company Setec OY, which completes the ePassport and sends it to the recipient. The final distribution of the ePassport to its owner is made by conventional mail.

The US system is somewhat different [35]. The first time a citizen applies for a passport, he or she must apply in person at a facility, which performs passport acceptance. These include Department of State's Bureau of Consular Affairs, Office of Passport Services/Customer Service, i.e. several post offices, clerks of court, public libraries and other state, county, township and municipal government offices. The person must fill out the "Application for Passport, form DS-11", present proof of US citizenship and proof of identity, provide two passport photos, a social security number and pay a fee.

This part of the system is similar in nature to the Norwegian one. However, if a citizen wishes to renew his or her passport, and certain criteria are met, all that is needed is to fill out the "Application For Passport By Mail, form DS-82" and send it by mail in a padded envelope along with his or her most recent passport, two identical passport photos and a fee.

The Norwegian Data Inspectorate, the body responsible for nationwide adherence to the Norwegian law of Personal Information is the institution that has directed the harshest critique against the ePassport in Norway. In some areas, the Norwegian Data Inspectorate is the Norwegian counterpart to the US' American Civil Liberties Union (the ACLU). The ACLU however, is completely politically independent and has highly extended responsibilities compared to the Norwegian Data Inspectorate. The self-proclaimed responsibilities include protecting the individual's freedom of speech, association and assembly; the right to equal protection under the law; the right to due process; and right to privacy [5c]. The final point of the ACLU's tasks is the one corresponding to the tasks of the Norwegian Data Inspectorate.

There are several security issues in the Norwegian issuance procedure, as noted by the Norwegian Data Inspectorate in their report dated March this year:

15 November 2005, the Norwegian Data Inspectorate performed an inspection at the Norwegian National Police Directorate, which is responsible for issuing the ePassport. 16 March 2006, the report following the inspection was published [36]. In the report, the Norwegian Data Inspectorate pointed out several weaknesses in the routines of the Police Directorate, and several demands were made to improve security and privacy. The deadline to meet the demands was set to 1 May 2006.

The demands were (in short, freely translated and without paragraph references to the Norwegian law of Personal Information) as follows:

- The Police Directorate must develop a written agreement about the treatment of data with the outside parties used to develop and issue the passports.

- The Police Directorate must perform necessary risk evaluations.
- The Police Directorate must provide both applicant and holder of the ePassport with proper information about the applicant's rights regarding acquiring knowledge about, correction and deletion of personal information.
- The Police Directorate must provide both applicant and holder of the ePassport with proper information about how the personal information is treated at points of entry in Norway, and how the ePassports may be expected to be used at points of entry in other countries.
- The Police Directorate must develop and implement a system for internal control.

The ACLU has also had its share of critical comments to the ePassport. Among other things, the organization disclosed the fact that the RFID chips originally intended to be used had a reading distance of about 30 feet, or 9 metres. This was of course unacceptable, and new RFID chips had to be implemented. Additionally, the ACLU protested when the US government planned not to encrypt the digital information in the RFID chip, stating that this made it possible to create bombs that only explode when close to a US citizen. The protests from the ACLU have resulted in both the ICAO and the US government changing their implementation choices.

7 Other Use of the ePassport and its Components

Passports are primarily used for immigration purposes, as identification of any person who wishes entry to a country other than his or her own. Other parties have, however, taken to use the passports themselves, both as a means of identification and to ensure payment or secure outstanding debits, often from foreign customers. These parties include hotels, cruise ships, Airplane check in and other, private parties. The practise is by now more or less commonly accepted, although many people dislike parting with their passport, especially in countries with a rather shady reputation. Despite of these reservations, some believe that the ePassport may become popular in e-business.

Also, for Norwegians, the passport is the only accepted identity document outside of the Nordic region [37, art. 2]. This means anyone who requires identification from Norwegian citizens may demand to see the passport. In essence, any bar, pub or other establishment serving alcohol outside of the Nordic region would than have access to personal information, especially that of younger citizens.

When ordering tickets for the UEFA Euro 2004 in Portugal, European citizens had to provide their name, date of birth, number of their passport or of the ID-card and date of passport issue into an Internet form [38, p. 10]. This information is exactly the one needed to derive the Basic Access Control key. This is a major cause for concern, because if the algorithm for deriving the key becomes public knowledge (distributed on the Internet by hackers), anyone succeeding in retrieving this information is able to read the information on the ePassports RFID tag. This procedure will also be used for certain concerts, the “2006 FIFA World Cup Germany“, the “UEFA Euro 2008” in Austria and Switzerland and the Olympic Games or other athletic world championships.

Another field of application for fingerprints or other biometrics is as identification or authorization keys in personal appliances, or in private or governmental security systems. Some of the systems that already apply fingerprint identification are private computers, car ignitions and door locks, access to physically sealed-off security areas in corporate or governmental buildings and access to corporate or governmental data, for example in databases. Certain security systems also use fingerprints as part of the access key, in addition to for example passwords and smart cards.

Figure 4 Fingerprint door lock

8 Control Procedures

The ePassport has been developed partly with a goal in mind that the immigration control of travellers to some degree can be automated. Exactly how automated the process will be is difficult to predict at present, but it will probably be cheaper and faster than the traditional manual control, and therefore is highly desirable.

Immigration control is the only point in the lifetime of the ePassport where it is guaranteed to be communicating with another entity, namely the passport reader. This communication has been subject to much discussion both in the media and by security and privacy experts. Early reports from experts told that expected communication range was about 10 metres. In other words, a hacker could be 10 metres from the passport with a reader and get the information from the tag. These reports have been to some degree silenced, as new RFID tag specifications have been implemented. At present, about 30 cm is the maximum expected possible reading range [36].

At present, passport control personnel have been required to know the characteristics of any country's passport to successfully detect and stop frauds. The ICAO passport standard allows member states to choose much of their own passport designs, including security methods, given certain common specifications [9]. There are 189 member states, and each has a different implementation. Keeping track of all of the different passports, obviously, is not easy. A machine passport reader would probably do this job much easier and more accurate.

There are already machine passport readers in use, but these only scan the machine-readable zone. With an RFID reader the inspector do not have to put the passport on a scanner, it will be sufficient to hold it a couple of centimetres from the reader. Even though the inspector will still scan the machine-readable zone (MRZ) to use this as a checkpoint against the RFID chip, it will to some degree be timesaving. This is because the inspector does not have to take every passport into closer look.

Figure 5 Automatic passport scan

Several countries, and the EU, have signalled current and future use of both national and international databases containing personal information of all citizens holding ePassports. The personal information therein also includes biometric data; the same as the ePassport does. The database is then used to ensure the person holding the passport is indeed the individual he or she claims to be. A check against the database is made every time a person passes through

immigrations. In certain places, due to various reasons, the database may not be constantly updated.

The US is very careful whom they let into the country after the terror attacks of 9/11. Everyone that enters the country have to tell exactly where he or she is going and how long he or she is going to stay. Travellers, at least those without biometric passport, must give fingerprints when they enter the States, and their picture is also taken. This information will be stored in the database the US already uses to check the passport holders travel history. Everybody that enters the United States is checked against this database, and if there are some irregularities the holder is questioned until the inspector is pleased with the answers. If the inspector is not pleased the traveller has to leave the country, or, in some extreme cases, they will be put in custody until the inspectors, or other security personnel, can get more information.

9 Discussion

9.1 RFID and Biometric threats

In this chapter we will present general security threats against RFID and biometrics.

9.1.1 RFID Security Threats

In chapter 2 we introduced the STRIDE model [23]. We will now use this model to analyze the possible problems that could occur with an RFID tag.

1. **Spoofing identity.** Spoofing occurs when an attacker successfully poses as an authorized user of a system. In other words it occurs when an attacker impersonates other persons. In RFID that means that an attacker steals information from a tag and uses that information in another tag, or the attacker can use the original tag, to impersonate the original owner. Mostly spoofing is a term used about stealing an address or some kind of identifier. This information is then used in another tag to make it seem like the original one. The rest of the data does not have to be similar.
2. **Tampering with data**. Occurs when an attacker modifies, adds, deletes, or reorders data. When a tag is modified, data is changed to let the tag look like a "good" tag. That could mean that the serial number (or other identifier) is reordered to look like another tag. Adding data is a way to achieve the same thing as with modifying, but here data is added instead of changing already existing data. Reordering data can be used to achieve exactly the same thing.
3. **Repudiation**. Repudiation can be seen as denial by one of the involved parties in a communication of having participated in all or part of the communication. An example of this could be a reader in a system denying that it has received information from an RFID tag.
4. **Information disclosure**. Occurs when information is exposed to an unauthorized user. This is a breach of privacy if the information is about an individual, as it is in passports. An attacker can use a reader to read the information on a tag that is nearby, or similar kind of attacks.
5. **Denial-of-service**. Occurs when valid users are denied service. Mostly used to block readers from reading a tag. Can be used in an attempt to steal a product that is marked with an RFID tag. In passport control this can only be used to force manual control.
6. **Elevation of privilege**. Occurs when an unprivileged user gains higher privilege than they were originally authorized for. Users can become attackers if they raise their status in the information system (database) connected to the reader in an RFID system.

Not all of these threats are as dangerous to ePassports as it is if RFID is used for product tracking. When it comes to ePassports it is important that users' privacy be protected, and that it is difficult to steal another person's identity either by spoofing or by tampering with data on tags to pose as another person. It is unlikely that an attacker will try to just modify a chip or spoof identity, but we can imagine that it is more likely to combine these attacks. For example, an attacker can steal information from a tag (spoof) and modify another tag they possess to impersonate the original tag. The difficult part for an attacker is getting the information in the passport book to be similar to the information on the tag.

Information disclosure is the most dangerous aspect of security around ePassports. In a world with widespread terrorism it is possible that terrorists or other criminals will try to kill people based on their citizenship. It is also more or less possible for governments to watch over potential terrorists if it is easy to read the information, even though this is not such a big new

threat, as governments already have ways to watch over people. In other words we can say that it is important that privacy is protected.

As mentioned before, one of the new threats to RFID is computer viruses. A virus can be implemented on a RFID tag. This virus could be a member of three categories; buffer overflows, code insertion and SQL injection. When the reader gathers information from the tag, the virus will attack the software (the database or other) that the reader is connected to. The virus will then be implemented into other tags that communicate with that software, or the software will not function, as it should. These threats are not of a big concern when it comes to the ePassport itself, but can in some way be involved with the control procedure. This is based on the assumption that it is possible to add or change data on the RFID chip after it is implemented in the passport. The chip is write-secured when it is implemented in the passport, as this is one of the security features, but we do not know what will be the case later, if digital visas are to be implemented as indicated.

9.1.2 Biometric Security Threats

It is possible to fool a face scanner simply using a picture instead of a real face. This is mentioned in [8], the main report we used for our initial literature review. Of course, if a guard is present and ensures the actual face is scanned, this should be prevented. High quality facemasks might be a more difficult matter, but demands rather good access to the face one wishes to copy. As the face does not contain very many, highly unique characteristics, the face recognition systems actually have an error rate of 5-40% already [10], making them insecure enough without active attempts of fraud.

A larger fraud problem appears when using fingerprints. It is actually quite easy to produce false fingers or fingerprints on films that can be attached to the finger [26]. Taking copies of fingerprints is only slightly more difficult without the cooperation of the owner of the finger than with cooperation. One only needs the fingerprint on a smooth surface, like glass or metal, or the finger itself, which we find a more inhumane way, although tough criminals probably find it quite convenient. This attack is actually difficult to detect even when guards supervise the process in its entirety. Also, it is statistically possible, yet less likely than with facial recognition, to be identified as another person due to the somewhat restricted number of minutiae used. The use of pulse detection might counter the use of false fingers, but might not detect the use of fingerprints on films.

We would believe that iris scans, which are regarded as the most secure biometric, may be vulnerable to similar attacks as the fingerprints, using contact lenses with the desired patterns. Some may claim the tendency conventional lenses have to move around the horizontal axis changing the position of the pattern will make this difficult, but this problem is already solved by the contact lens industry itself, making the “bottom” of the lens heavier than the top. This technique is already quite successful in contact lenses using certain patterns like cat eyes and “smileys”. To acquire the pattern however, one must have access to the eyes of the individual the attacker attempts to impersonate, either at close enough range to take a photo of the iris, or by removing the eye itself, grotesque as it may be.

The use of biometrics is not as free from problems as one might think at first glance. Facial recognition is made difficult when a face is disfigured by some accident. Fingerprints cannot be taken from people who do not have fingers, and iris scans are useless if the eye has been injured or infected with certain eye diseases making the cornea opaque, destroying the patterns of the iris or in other ways preventing iris scans. How individuals with these

challenges are to be identified may in fact be a security problem. Suppose a criminal burns of his or her fingerprints to avoid the identification process, how can this be counteracted?

On the other hand, fingerprints may disclose information that is highly private, and protected by privacy legislations. According to some research, various papillary patterns may have correlation with some diseases [38]. It is said that certain papillary patterns are dependant of the nutrition of the mother in the third month of the pregnancy, and leukaemia and breast cancer might be statistically correlated to others.

We will not discuss whether it is likely that certain papillary patterns are correlated to certain diseases, we simply state that we do not believe it impossible. Both may be influenced by genetics, and as some genes are correlated to others, the scenario probably needs serious research. If this is indeed the case, this is definitely very private information and should be particularly rigorously protected. The information would probably be very interesting to insurance companies and potential employers, but should be kept private.

9.2 Discussion of The ICAO Standard for ePassports

Development of the standard has become a lengthy process. Doc 9303 is a relatively large document with many different aspects to consider. It is important that the ICAO standard is a standard that all members can follow, and therefore everything has to be thoroughly revised and reconsidered. The fact that Part 1 of the standard has not been updated in a full scale since 2003 interprets that the work is thorough. The TAG/MRTD has had conferences to work through some of the problems. They have also had a good exchange of updated or commented supplements to Doc 9303 among the members of the group. We believe that this kind of cooperation will give a good result, as we will probably see in the new version of the document.

The ICAO standard is just a guideline for what features that could or should be implemented. There are few required features. This results in very different choices in different countries. We find the standard a bit poor in the sense of being just a guideline not a set standard the members have to follow. It will be better with electronic control than manual, but this can still create some problems. More about this issue will be discussed in chapter 9.6.

The current issue of Doc 9303 Part 1 contains extremely little about digital security. Mostly it is security related to the issuance of the passport and the layout of the pages. Security must be a larger part of the new standard, as integrated circuit cards and biometrics are implemented in the passport. Security aspects must now consist of methods against attacks against the RFID tag when the passport is in an immigrant's pocket, or when it is presented to the reader. Layout of the pages has to be an issue even though the RFID part of the passport is the most important aspect. The reason for this is that there are several countries that are not a part of the ICAO, and therefore they don't have the same security methods, and possibly no RFID implemented.

9.3 Discussion of National Implementation

Since there are many different security methods that possibly can be implemented in national passports, there are many problems a nation may face. The problems can be with the passport, with the reader or with the software the reader is connected to. Problems with the passport can be; issuance, activation of the RFID chip, encryption and other security methods on the chip, or it can be to figure out which information that should be stored at the chip. Problems with the RFID reader could be; long scanning-time, difficulty to use, wear and tear on both reader

and passports, and stability problems. The software has to contain a database, and therefore there could be security problems connected to this. Especially if the database is a central base which clients have online connection with.

If we look closer at the databases to be used for identity check, there are at least as many threats to this as any other database connected to some kind of network. Encrypted direct lines between the clients and the database will keep some of the threats at a pleasant distance, but there are still other things to consider. It is highly important that this database is protected against hackers, because the database will contain highly sensitive information. Information can be things like name, address, personal number, criminal records, where the holder has been, and where the holder is going to travel. An international database is not a national implementation problem, but the security of the clients connected to the database is. Every time a passport is read the clients makes a query and sends this to the database. If an attacker can hack into the client he can send queries, or he can read the information that is a part of the query. This information could be sufficient to get the information the attacker wants.

A lot of the countries have implemented a database of their own. Indeed many countries will probably choose to only use their own database until an international database of sufficient quality is presented, which will probably not happen until most of the countries have the same biometric implementations. One of the most well known databases is the American one. This database is mentioned in chapter 8. The database used in America has information about the holder, including biometrics, and the holders' travel history. It will also have some information about criminal records. When a national database, like the American one, is implemented, the security aspects of clients in the network are as important as if it was internationally implemented. The American national database must also be a security issue for the American government, and security methods have to be implemented for the database itself.

Also, the different implementations of national and international databases create a security problem for those choosing not to use a database for verification of immigrants and passports. The fact is that a fake ePassport is less likely to be detected in a passport control situation, as it will not be compared to the records of any database. Hence, organized criminals like the mafia would probably prefer to falsify passports from countries using neither a national nor international database.

Readers are another implementation issue. How the reader works and which design it has is not a government issue. The government has to buy this from a manufacturer they find trustworthy, and that delivers user-friendly, fast and reliable readers. The most important thing about the reader is that it is reliable.

The most important implementation issue the countries are faced with is the implementation of the passport itself. If RFID is implemented, all the other aspects mentioned about the database and the reader must be considered, if not, countries do not have to take this so much under consideration. Many countries will probably implement a database even though they only have machine-readable passports.

The issuance and some security aspects of the passport is presented in chapter 6 and discussed in chapter 9.4. The other aspects of the passport implementation we will discuss in some degree here.

The ICAO has not set a date for implementation of RFID. All member-states have to implement the machine-readable zone by 2010. Even though the ICAO have not argued that all members have to implement RFID and biometrics, it is more secure so the ICAO will most likely urge implementation to commence as soon as possible. More than 40 countries have given notice that they will implement it by the end of 2006. We believe that with this frequency of countries implementing RFID and biometrics in their passport, most of the ICAO member-states will probably have these features in their passports by 2010, not only machine-readable zone. In Scandinavia all countries will have the ePassport in use from 1 August 2006.

The reason several governments have chosen to keep the ten-year lifetime for passports, is, we believe, economics. A Norwegian passport now costs NOK 990, and a US passport costs USD 97. The governments probably fear that citizens will protest if faced with such fees every five years or so. To some degree, we understand this, and it will probably also cost the governments increased sums if shorter lifetime results in more development. However, there are very serious security and privacy risks, not to mention technology performance issues, in pursuing a ten-year lifetime, as we have described in chapter 5.

9.4 Discussion of Issuance

A good place to start this part of our discussion is by focusing on the five demands from the Norwegian Data Inspectorate to the Norwegian Police Directorate. In our opinion, all governments issuing not only ePassports, but also passports in general should seriously consider these.

The first demand was: “The Police Directorate must develop a written agreement about the treatment of data with the outside parties used to develop and issue the passports.” In the report, Setec OY was especially mentioned, as the company as far as we understand inserts personal information into the passport both physically and electronically. The Digital Signature key used for Passive Authentication is supposed to authenticate the issuing government, but in reality, is it actually used by Setec? In [36, p. 7] the Data Inspectorate states that during the inspection, the Police Directorate informed that the electronic contents of the ePassport was secured with a so-called “root key”, and that this key is in the possession of the Police Directorate.

The “root key”, we assume, is another name for the digital signature key, which is a private key in a PKI. If so, the Police Directorate is responsible for the correct use of the key. At the police information webpage for ePassports [37, art.1] it is informed that all personal information is sent electronically to the Norwegian Setec subsidiary in Oslo, which in turn engraves it in the ePassport and then sends the ePassport by ordinary mail to the recipient. This means that Setec also must be in possession of the key, and using it. As we have not been able to obtain the written agreement between the Police Directorate and Setec, we do not know what rules exist for how Setec must treat this extremely sensitive piece of information, but we of course share the concern of the Data Inspectorate over the shortcomings of the written agreement.

Setec will also treat all personal information of ePassport applicants, in all three Scandinavian countries. This probably makes it a very interesting target for individuals with malicious intents. To some extent, using decentralized subsidiaries in each country in which Setec is responsible for developing and personalizing ePassports probably counteracts this threat. We believe this is one of the key motivations for Setec to establish daughter companies in

Norway, Sweden and Denmark. The other reason for decentralized personalization of the ePassports is of course that it is easier and probably cheaper to perform this task in the respective countries. We would not be surprised if the governments actually require that ePassport personalization be done in the respective country due to security and privacy considerations.

Also, we do not know what security routines Setec OY employs. With our best efforts, we cannot find that the Setec website contains very available information about company internal security. Of course, we believe that this more than hundred-year old company has very good routines. However, any company is in essence no more than a group of people and their collective resources. We are certain that company culture and formal procedures are highly security-conscious, but no system is completely foolproof. To believe anything else is naïve and very dangerous. Our concern is that individuals with malicious intents might gain access to sensitive information. We find it necessary to emphasize that we do not suspect Setec OY of inadequate security measures, the company has long traditions in the security printing business, and the list of partners and customers is both long and impressive. We simply state that any company might become compromised, and this should be kept in mind.

The second demand from the Data Inspectorate was: “The Police Directorate must perform necessary risk evaluations”. According to the Data Inspectorate, several areas of the issuance process need risk evaluations, which are used to discover security threats and security levels. The Norwegian law of personal information, which demands systematic efforts to achieve proper protection of personal information, supports this demand. By September 2005, The Police Directorate had not performed any risk evaluations.

In general, the Data Inspectorate expressed concern that the information security choices are based on several documents, both official [9] and unofficial [24,27,30,39,40,41], from the ICAO. The Data Inspectorate feels there is some confusion because some of the ICAO security measures are required while others are recommended, and that the final decisions regarding which to incorporate are unclear.

We found certain parts of the Data Inspectorate report unsettling. Some of the statements made by officials did not completely coincide with views made by experts, or did not express enough concern for relatively well-known risks. This was especially the case when discussing the Basic Access Control and expected lifetime of the ePassports. We chose to question the Data Inspectorate about certain of their statements. The e-mail we sent to the Data Inspectorate and their response is presented in Annex C.

We asked about whether they really regarded BAC to be secure enough, as they seemed to accept as a fact in the report. We also asked why they seemed to mean that a visual inspection of the photos to be used against the applicant was poorer than using biometric identification algorithm on a computer. Earlier in this paper we have cited UK experts who claim machines are potentially even poorer at recognising faces than humans. Finally, we asked them to outline what a risk evaluation is supposed to produce in terms of solutions. The answers to these questions will be presented where appropriate.

We did discover one fact about the Norwegian Data Inspectorate. They do not approve or disapprove methods to be used for securing ePassports. This is the responsibility of the Police Directorate. The only means the Data Inspectorate has at its disposal to point out poor choices

is demanding risk evaluations. We believe the Data Inspectorate demands risk evaluations to force the Police Directorate to discover when a method is not sufficiently secure.

The Different areas and methods that need to be risk evaluated are discussed in the 15 following paragraphs.

First, the issuance procedure of sending the ePassports by conventional mail is mentioned. There is no way to ensure the correct recipient receives the new ePassport. It is also possible to intercept the passport by taking it from the mailbox, keep it for some time and then put it back. This method is, we realise, quite cumbersome, and the main problem is how to know who has applied for a passport, and when it will arrive. Observing police station activities, and perhaps stealing the wallets of applicants to determine their identities might achieve this. The method is unlikely, but probably not impossible, and we also believe organized criminals have more experience devising creative plans to steal passports than us.

The Police Directorate argues that sending them by registered mail would cost NOK 19-20 million per year [37], so this according to them is out of the question. Another solution might be the passport applicant having to personally retrieve the ePassport at his or her respective passport issuance facility, i.e. the police station. Alternatively, the postal office could be used for this, but we do not know at what cost.

Secondly, the Data Inspectorate demanded risk evaluation to be performed on the lifetime validity of the ePassports. At present, the effective lifetime is set to 10 years, just as for the old passports. This, we believe may be of serious concern. It is not extensively debated in the report, but in our opinion, it is dangerous to guarantee a relatively new technology using cryptography to be sufficiently secure for such a long time.

In this concern, the popular Moore's law plays an important role. It states that the complexity of integrated circuits, with respect to minimum component costs, doubles every 24 months [29]. This means that, put very simply, every two years computers double their strength and calculation capacity. It was stated in 1975, and has been predicted to fail several times during the years, but has in general held the test. Moore's law is an empirical observation used as a prediction, and as such it may very well be a self-fulfilling prophecy. In any case, the fact that computing capacity increases at such a rapid rate, gives us some concerns.

For starters, the RFID chip is one such integrated circuit. If it is to follow the rapid evolution Moore's law predicts, it might be clever to wait only a few more years until the chip storage space is somewhat larger and can include heavyweight security measures, at no or little added financial cost. But the fact that computers used for cracking encryption codes also evolve is more sinister in nature. This means that in ten years time crackers might with some effort be able to break the security of the ePassports.

Another concern regarding the long lifetime of the ePassports is in the fact that encryption algorithms face serious attacks from both scientists and hackers/crackers. The goal of the former is to attempt to prove or disprove the security level of the algorithm, and the goal of the latter is well known. Several so-called secure algorithms have met their demise during the years, toppled over by some unknown mistake. We fear that in time some security algorithm of the ePassport might face this fate.

The different security measures using ciphers that are used by the ePassport RFID chip are: Passive and Active Authentication and Basic Access Control, BAC. Passive and Active Authentication use one of the ciphers RSA, DSA or ECDSA for Digital Signatures. BAC uses two-key triple-DES in CBS mode. We will in short present the security level they at present hold. RSA and DSA are widely used ciphers, and are regarded as secure if the keys used are sufficiently long. ECDSA is a variant of DSA, producing smaller key sizes for the same security level, while execution time is roughly the same and signature size is unchanged.

The ciphers are all using one private and one public key, which some attack types might be able to break. Breaking a cipher may however mean two things: obtaining the message itself or achieving the secret key for enciphering and/or deciphering. Primarily, we consider the situation where an attacker uses eavesdropping equipment to intercept the communication between a passport and a legitimate reader.

The first possible attack against a public key system is a “Forward Search”, or precomputation [42]. A Forward Search attack exploits limited input message entropy, when using the public key to encipher information only intended for the secret key holder. This requires that the attacker actually possesses the public key. As it is not a secret, the public key might be available at present or at a later time. Forward Search however, does not result in achieving the private key. It simply provides a possibility to discover the original message through comparing the cipher text to already enciphered possible messages (hence the need for a limited input message entropy). Active Authentication also includes random padding data, probably intended to counteract this attack [8].

DES is clearly the weakest cipher of the group. In its original form it is possible to break in less than 24 hours [29]. However, the version used in the ePassports is much more complex. It uses two keys and three subsequent encryptions (or encryption-decryption-encryption), making the encryption much more secure than single DES. However, two-key Triple DES is vulnerable to certain “Chosen Plaintext” or “Known Plaintext” attacks, which in worst case could reveal the secret key. Both attacks require the public key to be known, and we do not at present know how easy it will be to achieve it. In addition, the encryption is in CBC mode, meaning that the previous cipher text block is used to scramble the next plain text block. To counter this, an attacker would need to know the initiation vector, which is stored along with the keys.

We find it quite clear that given enough time, these attacks are much more feasible. The scenario of a hotel or cruise ship holding the passport for the entire stay of a tourist is a much more likely attack situation. The entropy of some of the messages between the passport and a reader is not very large, so forward search, chosen plaintext or known plaintext attacks may succeed now or later, especially given the evolution of the hardware needed to perform the calculations.

The third area the Data Inspectorate demands to be risk evaluated is the BAC itself. The Police Directorate claimed BAC to be sufficiently secure, but the Inspectorate still demanded risk evaluations. At this point, we discovered what the Data Inspectorate really meant about the use of BAC. According to Atle Årnes, a senior engineer at the Data Inspectorate, BAC is not a good algorithm, and the main problem is that the information to derive the keys is not a secret. It is contained in the machine-readable zone, and is among other things used for ordering tickets for large happenings like international sports arrangements and concerts. The

Data Inspectorate hoped the Police Directorate might also realise this through a risk evaluation.

The fourth area requiring risk evaluation was the reading distance of the RFID chip. At present, the distance is about 10 cm when using BAC. Without BAC, the distance might be 30 cm. As the RFID chip is passive, its transmission power is limited. However, simple eavesdropping on the communication is already possible from much larger distances. The limiting part is the error-correction equipment, which may very well experience considerable development during the next 10 years. It is necessary to note that using a Faraday Cage prohibits communication except when the passport is open. However, nobody has any control over what future situations that may require the passport to be open, so in our opinion this is actually only a way of making it a bit more difficult to gain access to the information.

The final area in which risk evaluation had to be performed was the gathering of data from the applicant. The two pictures to be provided by the applicant was the most serious concern. There is no guarantee that the pictures actually are of the correct individual, and at present, only a visual inspection of the photo is made. The Data Inspectorate argues that in Sweden, the applicant has to take the pictures at the police station, ensuring the validity of the picture. The Police Directorate states that this is too expensive, and not feasible. The Data Inspectorate, as we mentioned earlier, questioned the visual inspection, because, again according to Atle Årnes, only a machine can compare biometrical data with biometrical data. We tend to agree, as only a machine "sees" well enough to count pixels between the eyes, for example.

At some later stage, the Police Directorate will probably implement the same method for biometrics identification as immigrations control, and then, supplemented by visual inspection, the identification will probably be "good enough".

The third demand from the Data Inspectorate was "The Police Directorate must provide both applicant and holder of the ePassport with proper information about the applicant's rights regarding acquiring knowledge about, correction and deletion of personal information." The law of personal information demands any citizen be given the opportunity to view and correct any personal information gathered about them. This also applies to the information contained in the RFID chip of their personal ePassport. However, this can only be accessed through special readers, and at the time the report was written, the only readers in Norway were in the possession of Setec and "Politiets Data- og Materielltjeneste", PDMT (directly translated the "police's data- and materiel service"), and not available to the public. This was not acceptable, and now, readers are available at all police districts.

The fourth demand from the Data Inspectorate was: "The Police Directorate must provide both applicant and holder of the ePassport with proper information about how the personal information is treated at points of entry in Norway, and how the ePassports may be expected to be used at points of entry in other countries." When the report was written, very little – and even self-contradictory information was available to citizens about the information contained in the ePassport and what security measures were used. The Data Inspectorate required this information to be available on the police website. Since the report was published, this has been improved greatly, but we still claim the Norwegian Police Directorate should have studied the websites of our Scandinavian counterparts Sweden and Denmark, and learned much about informing the citizens.

The final demand was: "The Police Directorate must develop and implement a system for internal control." At the time of the inspection, the Police Directorate admitted to lacking internal routines, and we can present two local examples of this. First, the grandmother of one of us actually received her last passport with the last name of another woman written in it. The explanation was that the mother of the officer writing down her information had the same first name as her, and therefore automatically wrote his mother's last name.

Second, and more serious, at 7 May 2006 the local newspaper Agderposten [43] wrote an article about a man who received his new ePassport with the picture of a completely unknown man. He found this quite odd, as he had himself witnessed the officer attaching the correct photos to the application form.

Several good practice advices exist, and one of the most important is the principle of Separation of Duties [4, p. 152]. In short, this principle states that if two or more steps are needed to perform a critical task, then at least two different people should perform it. This principle is closely related to the fact that redundancy is a way to detect and prevent errors like the two we presented above. Redundancy is accomplished by letting another person check that the information recorded is indeed correct.

Another possibly useful principle is the one of Economy of mechanism [4, p. 344], stating that security mechanisms should be as simple as possible. The principle is easy to project to any type of mechanism, and is correlated to the KISS (Keep It Simple, Stupid) principle. It is well known that simple procedures result in fewer errors. At the very least, the Belgian passport issuance procedure should be studied, as this country seems to be regarded as one of the best in security and privacy issues.

Any government issuing ePassport should seriously consider these concerns. However, other governments use even less secure procedures for issuance. US citizens meeting certain criteria may actually apply for new passports by conventional mail. This means no check is made to ensure the photos are correct, nor that the person actually has requested a new passport. We find this very disturbing, for obvious reasons.

9.5 Discussion of Other Use of the ePassport and its Components

As we have already noted, it is by now more or less commonly accepted that foreign hotels and cruise ships require the possession of their visitors' passports, either for some time or for the entire stay. This is to ensure payment, but also provides the hotel or cruise ship owners and employees access to private information. While eavesdropping on legitimate communication between passport chip and reader, which is a commonly mentioned and dreaded hacker attack, faces the difficulties of having to be performed on real-time information flow, an attacker having access to passports in this scenario could have a full week or longer to complete his or her attack.

As most people already know, many young people do not worry much about anything, especially when partying on vacation in another country. It is not difficult to believe that they would gladly present their passport if required upon entering a bar. Often, adults are more careful, but might also be persuaded. Suppose the bar then offers to take care of the passports for their customers, maybe in "safe" deposit boxes. This would provide the owners with complete access to the passports for a night, given that they simply possess a spare key and keeps an eye out for when the passport's owner wishes to leave.

Facial recognition was originally adopted as primary biometric identifier in the ePassport largely because the face is the biometric most citizens already display in public. As previously mentioned, the facial features is what most humans use to identify other individuals, and is also the preferred biometric used in most ID documents. However, many of the ICAO member states (the US and EU for instance) either already, or will at a later stage, demand the use of additional biometrics identifiers, particularly fingerprints.

The use of fingerprints in ePassports might be problematic in regard to other areas of applications for fingerprints. Concern has been voiced that citizens may not wish to provide their fingerprint as a second biometric, because they know the police use fingerprints when identifying and processing criminals. One obvious area where fingerprints are used for identification is criminal processing, as most countries have a national or international database containing fingerprints and other personal information belonging to criminals. This means that it is theoretically possible to check the fingerprint of any traveller to see if he or she is indeed a convicted criminal, even without the person knowing of it.

The obvious place to perform this check is at immigrations control, but people with the correct access may do this almost anywhere. All that is needed is a passport reader. One may argue that the 'Faraday Cage' on the passport covers will protect the information, but consider what happens when visiting a foreign hotel or cruise ship, as mentioned above. The passport is left in the reception, sometimes for the entire stay. The hotel will argue it is a insurance that the bill will be paid, but it also gives the staff ample time to investigate, and, if they have malicious intents, copy the passport itself or parts of it.

The threat increases if, as the EU Data Protection Working Party [37] fears, the algorithm of the BAC key creation becomes publicly available on the Internet. As the expected effective life of the ePassport is 10 years, this is definitely possible.

We can only assume that most citizens and private companies do not approve of governments having access to all or part of their access keys to secret data or protected facilities. Even foreign governments gain access to the data if the person ever visits the country. There is no limit to the lifetime of biometric data, especially fingerprints, so any government that has ever processed the person through immigrations in practise possesses his or her biometric data. There is very little clarity on how the biometrics databases will be protected from attacks, especially if an international database is to be used. This fact is not settling for anyone, and will probably be the seed to several public discussions and much frustration, we fear.

9.6 Discussion of Control procedures

In manual control every inspector needs to know about the security methods different countries have implemented. At least they need to have good enough overview to spot any fake passports. With an RFID tag in the passport the reader will connect this to a database. In that way the inspectors just have to be aware of anything suspicious, like if the holders information is not exactly the same in the passport book and the chip. It does not mean that the inspector does not have to look at the passport book for any security features that seem not accurate, but it does mean that it is more difficult to make a fake passport. You cannot simply change the picture anymore, because the RFID chip will contain the original one.

The control procedure is outlined in Figure 6, taken from the ICAO "Biometrics Deployment of Machine Readable Passports"-report [24].

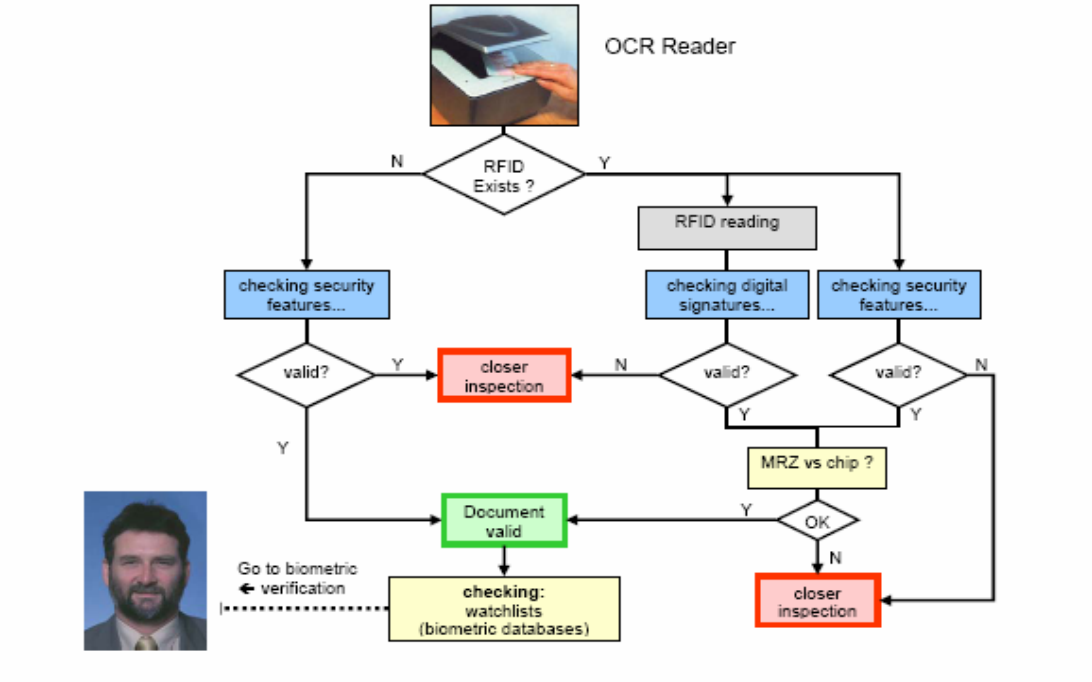

Figure 6 Typical Business Process of reading ePassports.

This figure shows that if no RFID exists in the passport there a standard manual control will be initiated. If the document is valid the passport will be checked against a database (like the American one) to see if there is any irregularities. If the document is not valid a closer inspection will be done.

If an RFID tag exists in the passport, one of two things will happen. Either the passport is presented to an RFID reader, or there is a manual check of security features. When a manual check is performed the passport will be deemed valid if nothing else suspicious appears while it is scanned as an MRP. Specifically, the data page, passport covers and the passport in general are inspected. When the passport is presented to an RFID reader, digital signatures will be checked. If these are not valid a closer inspection is preformed, if they are valid the MRZ will be compared with the information in the chip to see if there is anything suspicious there. If everything is OK the check against the database (watch list) will be performed, if something is strange the passport will again be inspected closer.

10 Conclusion

10.1 RFID and Biometrics Conclusion

RFID is the most important, discussed and well-known system of all automatic identification (Auto-ID) systems. During the last decades constant development of new applications of RFID has occurred. In ePassports, RFID is used for two reasons, more or less automatic scanning and the possibility to add biometric features in the passport.

There are many challenges with RFID. Fortunately the area has been under lot of research the last years. RFID is mostly used to identify products in warehouses and in stores, so the chip is mostly tested for this type of application. Even though there are some differences between the uses when it comes to product identification and ePassports, there are several equalities as well. There has been a lot of research around the security aspects for RFID, so the technology becomes more and more secure. Most of the security methods used in product identification can also be used in passports. The main difference is that the data the chip contains are more important in passports. Therefore it is more important that there should be some kind of encryption in passport chips.

Biometrics is a very good way of identifying individuals, as it does not require people to remember any passwords or tokens. An almost completely secure means of identification is always with them. However, even though most scientists believe that no two fingerprints or iris patterns are alike, the technical measuring equipment we currently possess is not yet exact enough to fully take advantage of the huge entropy of biometric characteristics. This means that errors may occur and false acceptance and rejection rates must be seriously considered. In addition, care must be taken to avoid the different types of attack the shortcomings of the computerized systems actually have. Finally, we urge that biometric information is protected sufficiently both in the ePassports and the corresponding database records.

10.2 Conclusion for The ICAO Standard for ePassports

The internationally applied standard for ePassports has been developed by the ICAO 'Technical Advisory Group on Machine Readable Travel Documents', or the TAG/MRTD for short. The ICAO standard for machine-readable passports (MRPs) is outlined in a document called "Doc 9303 Part 1 for Passports". This has not been updated since 2003, and the next version will come in two volumes. Volume two will contain the specifications for an enhanced MRP with biometric data encoded in a contactless integrated circuit (RFID) chip.

As mentioned in chapter 9.2, the standard has to be well revised and considered. We feel that the ICAO TAG/MRTD group has done a relatively good job here, even though the standard has received much criticism from experts within security and privacy. The fact that part 1 of Doc 9303 has not been updated in full scale since 2003 interprets that the work is thorough, and that all inputs have been taken to consideration, though we find it alarming that the experts in the TAG/MRTD group have not been more critical themselves. A lot of the problems that has surfaced after implementation of ePassports could and should have been avoided.

The standard itself is not updated that often, but the standard is based on many technical and non-technical reports. These have been updated fairly often. Especially the Supplement to Doc 9303 has been updated more or less continuously. The updating process of this document has been based on comments to Doc 9303 and the supplement by all TAG/MRTD member-states. We believe that this kind of cooperation will produce a good result.

The most negative aspect about the standard is that it is just a guideline. The fact that the standard is more a guideline than a set standard results in different choices of which features countries are implementing. We believe it would be easier and better if all countries implemented similar security features and similar appearance features in the ePassports. At least it would make it easier to control the passports all over the world.

10.3 Conclusion for National Implementation

We have mainly focused on the US and Norway, and one of the reasons are that the United States started work on their ePassports earlier than any other ICAO member. That have resulted in several rounds with experts, the public and privacy organizations. Norway is the third country in Europe to implement biometrics in their passports, and can be seen as pioneers in this context.

There are many aspects that must be considered before implementing ePassports. Security around the issuance and the use of ePassports is one thing, but it is most important that every individual's privacy is protected as well as a nations government can. With privacy we mean the ability to hide personal information from other than those the individual choose to give the information to.

The security of the international or national databases is one thing that has to be well thought of. If we look closer at such databases there are at least as many threats to them as any other database in a network. It is important that these databases are protected against the most usual attacks that appear in a network. They must also be secured as well as possible against hackers. If the databases come together to form one international, even global, database, the protection of this database has to be an international project. Even though the database itself is not a national problem for an international database, the clients connected to the database are.

The US has already implemented a national database. This database contains information about the holder; including biometrics and the holders travel history. It will also contain some information about criminal records. Anyone that enters the United States is checked against the database, and if there are some irregularities the holder is further questioned. This database is a direct result of the 9/11 terror attacks against the US. We believe that the Americans feel this enhanced security is the best way to stop possible terrorists, but citizens from other countries may find it a breach of privacy. Even though many citizens are against this, we believe that many countries will implement a national database. Even countries that only have machine-readable passports implemented will probably find a database useful.

Readers are, as previously mentioned, not a direct technical issue that the government in any country are responsible for. They are responsible in the way that they have to use manufacturers that are trustworthy. The reader itself has to be user-friendly, fast and reliable. The most important thing about the reader is reliability.

We see it as a good logic that as many countries as possible implement biometrics in their passports as soon as possible, hopefully soon after or at the same time as they implement the machine-readable zone (MRZ). As long as a country is an ICAO member, they have to implement an MRZ by 2010. We also believe that the ICAO will argument that because biometrics is more secure it should be implemented as soon as possible. Maybe most countries will have both an MRZ and biometrics within 2010. Even though using biometric passports creates a higher security level than conventional passports, there could be a lower

security level in the issuance procedure. Hence, we do not recommend that any country start implementing biometrics in their passport before they can issue it in a secure way. Some of the countries that have implemented biometrics in Europe are Sweden (1 October 2005), Norway (3 October 2005) and Belgium (November 2004). Denmark will implement ePassports for 1 August 2006.

10.4 Conclusion for Issuance

The Norwegian and US systems for issuance of ePassports differ in that US citizens who already have a passport and meet certain criteria may apply for a new one by mail, and do not have to do this in person. We seriously question the wisdom in this approach, as no definite confirmation of the application is made.

The five issues discussed in the report from the Norwegian Data Inspectorate are all current, and should be seriously considered by anyone issuing ePassports. First, the use of different private companies for development and personalization of the passports requires strict rules for what these companies are allowed to do or not, and what they are required to do or not. At the same time, it must be pointed out that the company does not have all the responsibility concerning security and privacy. The government is in the end responsible for everything and cannot transfer this burden to others.

Second, the use of risk evaluations both continual and at strategic points can uncover several issues to security and privacy, and should be rigorously pursued. Third, the general population needs information to feel safe and protected. If this is prioritized, much insecurity and frustration may be avoided. The information to be provided should include what information is recorded, how the information is treated, how to correct information if errors are detected, how the information may possibly be used both by the citizen's own government and others, and probably much more. Finally, the issuing authority must implement sufficient internal routines so that unnecessary errors may be prevented.

10.5 Conclusion for Other Use of the ePassport and its Components

Several parts of the passport are used in other situations than immigrations. Most individuals already have their names and birthdates, maybe even personal number in several databases with variable levels of security. Biometrics is used for identification and authorization in several private and corporate situations. Even the entire machine-readable zone is used for certain ticket ordering systems, making the data used for key generation in BAC much less a secret. This is a very serious concern, as the algorithm for key generation might become public if cracked some time during the next ten years. If this happens, BAC is practically useless.

Another cause for concern regarding other use of Biometrics is that governments will have access to biometric keys to private and corporate property and secrets. It is quite obvious that the EU will not recall the use of fingerprints as the second biometric identifier, even if citizens may protest both against the connection to criminal databases and because of the increased use of fingerprints as identifiers in personal appliances. How this problem may be solved is yet unknown, maybe through careful protection of the stored data. Also, the Belgian government already keeps a national database with personal information of its citizens [34], and a case study of what the government has done to earn its citizens' trust may result in a way to replicate the Belgian success

10.6 Conclusion for Control procedures

The ePassport has been developed with effective immigration control in mind. The control can to some degree be automated. At present, passport control personnel (inspectors) have been required to know the characteristics of any country's passport. Keeping track of all the different passports is a difficult job for the inspectors. A machine passport reader would probably do this job better and more accurate.

Machine passport readers are already in use, but many of these only scan the machine-readable zone. If RFID tags and biometrics are included in the passport, the inspection will go by faster than traditionally manual control. This is because the RFID information can be checked against the machine-readable zone and the information on the data page. With machine readers it will also be much easier to detect any fake passports. With an RFID chip or a machine-readable zone the passport will most likely be checked against a national or international database. This database will contain personal information about the passport holder, and in that way the inspectors just have to be aware of anything suspicious.

10.7 Overall conclusion

First, we find that the process of determining the specifics of the ICAO standard and different nations' implementations of optional security and privacy protection measures worthy of some criticism. For several years, serious security and privacy risks both caused by choices made in the standard and by individual nations have been detected, discussed and more or less improved. Several of these could in our opinion have been avoided if more attention had been paid to details. One example of this is that the use of active RFID tags would make it possible to scan personal information in them from outside the home of the owner. The inability of the ICAO and individual governments to create a satisfactorily secure system without considerable efforts from security experts and privacy organizations is disturbing, yet sadly not surprising. In our opinion, this is one of the ePassport system's most grievous flaws.

On the other hand, there are several other concerns, many caused by different choices in the national implementations. For example, implementing a national or international database containing the personal information of all citizens or pass holders would greatly decrease the risk of passport fraud. However, this security measure will compromise the individual's basic right to privacy unless serious constraints are made to the use of the database. We believe a study of the Belgian national database of all their citizens would provide guidelines for how such databases should be implemented, especially regarding the strict access restrictions, the extensive logging of any access to stored data and the citizen's right to access the logs containing information about access to his or her own information.

The Norwegian and US governments, among others, have both decided to set the effective lifetime for the ePassport to ten years. For several reasons, we find this to be a poor choice. As we have already mentioned in our "National Implementations" and "Issuance" sections, a ten-year lifetime causes many security, privacy and performance issues. A very serious concern is that RFID chips have never been tested for such a long time period, so there is no guarantee they will actually stay functional for ten years. Ten years also provides hackers and crackers with ample time to device methods to misuse the passports. The long lifetime seriously decreases the rate of improvement and further development of ePassport systems, which is a shame considering the rapid changes of both RFID and biometrics technology.

The ICAO itself explicitly recommends the lifetime to be only five years, and both Sweden and Belgium have chosen to comply. In essence, there are so many good reasons to choose

five-year lifetime for ePassports we hope other governments, including our own, will follow their example.

In general, we believe the ePassport system is closing on a secure enough level, but it is not quite there yet. We anticipate the next version of Doc 9303 and hope this document can produce more definite rules and guidelines. The countries that have already begun issuing ePassports may face somewhat critical issues if their security measures should fail, as we fear they might. The possible implementation of databases to support passport and identity verification may tip the scale in any direction. If sufficient privacy measures are implemented, this may be a valuable contribution to security, but if privacy is not well enough protected, the system will not be a success, as it will be difficult to implement worldwide due to privacy legislations.

It is as we predicted early in our project. Security and privacy do not counteract each other, but are intertwined for good or for bad. Both must be considered, as must the way they affect each other.

10.8 Further Work

We believe it important that attention be paid to the further development of the international and national ePassport system. The ePassport is here to stay, but we predict that several changes and updates will occur. One of the major issues now is the implementation of national and international databases for verification of passports and people. We believe these databases will be implemented, but only if sufficient security and privacy measures are applied. This work will be very important for the success or failure of the ePassport program.

References

All websites were visited on 28 May 2006, and were functioning at that time.

[1] The International Civil Aviation Organization, http://www.icao.int
The MRTD site, which provides information about the development of standards for Machine readable travel documents, including electronic passports
http://www.icao.int/mrtd/Home/Index.cfm

[2] The US Department of State travel.state.gov – web pages, giving information regarding travel to and from the US, and the Visa Waiver Program
http://www.travel.state.gov/visa/temp/without/without_1990.html

[3] Setec, manufacturer of the Scandinavian biometric passports.
www.setec.com

[4] Matt Bishop: *"Computer Security; Art and Science"*. 1. Edition. Addison Wesley, 2003.

[5] American Civil Liberties Union
http://www.aclu.org/passports
[5b] The ACLU letter to the US State Department:
http://www.aclu.org/privacy/spying/15306res20050404.html
[5c] About the ACLU
http://www.aclu.org/about/index.html

[6] The US Department of Homeland Security – web pages, giving information on the US-VISIT program:
http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0435.xml

[7] The Norwegian Security Authority, NSM's Web pages:
http://www.nsm.stat.no/

[8] Dr. Ari Juels, David Molnar, and David Wagner: *"Security and Privacy Issues in E-passports"*. SecureComm, September 2005

[9] Approved by the Secretary General: *"Doc 9303; Machine Readable Travel Documents – Part 1; Machine Readable Passports*". 5. Edition. ICAO, 2003.

[10] A BBC article including an interview with University of Cambridge - professor John Daugman, developer of the international algorithms used in iris recognition technology being tested by the UK Passport Service (UKPS). The article also includes a citation of Bernard Herdan, chief executive at UKPS:
http://news.bbc.co.uk/1/hi/technology/3389209.stm

[11] Letter to the Department of State from the privacy organization Privacilla.org:
http://www.privacilla.org/releases/RFID_Passport_Comments_2005-04-04.pdf

[12] Letter to the Department of State from the Samuelson Clinic at UIC Berkeley
http://www.law.berkeley.edu/clinics/samuelson/projects_papers/2005sp_electronic_passports_comments.pdf

[13] The comments provided regarding the new biometrical passports by US citizens
http://travel.state.gov/passport/eppt/passport_comments.php

[14] US department rule, publicized on October 25, also including an analysis of the 2335 comments received on the new passport ruling.
http://edocket.access.gpo.gov/2005/05-21284.htm

[15] U.S. Department of State Passport Agency publications.
http://www.state.gov/r/pa/prs/ps/2005/50927.htm

[16] Information about the Australian ePassport
http://www.dfat.gov.au/dept/passports/

[17] Oberthur Card Systems, the manufacturer of the Belgian and Thai ePassports, datasheet for the ePassports the company produces.
http://www.oberthurcs.com/downloads/datasheets/identity/epassport_1005.pdf

[18] German Research Center for Artificial Intelligent
http://www.dfki.de/~hutter/lehre/sicherheit/ss05/mrtd.ppt

[19] Cavoukian, Ann: *"Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology"*. February 2004.

[20] Brito, Jerry: *Relax, Don't Do It: Why RFID Privacy Concerns are Exaggerated and Legislation is Premature.* 2005.

[21] Juels, Ari: *RFID Security and Privacy: A Research Survey.* RSA Laboratories, September 2005.

[22] The International Organization for Standardization (ISO)
http://www.iso.org
The RFID handbook provided the specific ISO standards tied to the ePassports
http://www.rfid-handbook.com

[23] Dale R. Thompson, Neeraj Chaudhry, and Craig W. Thompson: *RFID Security Threat Model.* ALAR, March 2006.

[24] ICAO TAG MRTD/NTWG: *"Biometric Deployment of Machine Readable Travel Documents"*. ICAO, May 2004.

[25] Ton van der Putte and Jeroen Keuning, "*Biometrical Fingerprint Recognition: Don't get your fingers burned*". 21 September 2000

[26] Ulf Carlsen, "*Smartcard presentation part 2*", presentation in smart card technology and biometrics as part of the Computer Security Seminar subject ICT 506 at Agder Community College autumn 2005. The presentation was held at 15 September 2005.

[27] ICAO TAG MRTD: *"Annex I: Use of Contactless Integrated Circuit Cards in Machine Readable Travel Documents"*. May 2004.

[28] The "How Stuff Works" website: a very simple introduction to Face Recognition
http://computer.howstuffworks.com/facial-recognition1.htm

[29] "Wikipedia online, the free encyclopedia". When this website is referenced in the text, the current term has been searched for in the English version of the site. Be advised that Wikipedia is written collaboratively by volunteers, and errors may occur. We are aware of this, but have to the best of our knowledge searched the referenced texts for inconsistencies.
http://www.wikipedia.org/

[30] ICAO TAG MRTD: "*PKI for Machine Readable Travel Documents offering ICC Read-Only Access"*. October 2004.

[31] Mary McMunn (editor): *"ICAO MRTD Report"*. Vol. 1 No. 1, 2006.

[32] Swedish Police – About Biometric Passports
http://www.polisen.se/inter/nodeid=33373&pageversion=1.html
[32b] Swedish Police- About eID
http://www.polisen.se/inter/nodeid=33378&pageversion=1.html

[33] Danish Police - About Biometric Passports
http://www.politi.dk/da/borgerservice/pas/biometrisk_pas/

[34] Committee on the Judiciary
http://judiciary.house.gov/OversightTestimony.aspx?ID=352

[35] Travel.state.gov –Passports
http://travel.state.gov/passport/passport_1738.html

[36] Preliminary Report and warning about certain demands from the Norwegian Data Inspectorate, from the inspection at the Police Directorate on 15 November 2005. Report is dated 5 January 2006 and is available online, at
http://www.datatilsynet.no/templates/article____1351.aspx

[37] Norwegian Police Directorate's website
http://www.politi.no
Two articles are referenced, both from selecting "Pass, ID, attester" from the "Hva kan vi hjelpe med?" section
art. 1: "Jeg trenger nytt pass"
art. 2: "Jeg vil vite mer om Schengen-samarbeidet"

[38] The EU Data Protection Working Party: " *Opinion on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States*" (Official Journal L 385 , 29/12/2004 p. 1 - 6). Adopted on 30 September 2005

[39] ICAO: *"Machine Redable Travel Documents; Supplement to Doc 9303-Part 1-Sixth Edition"*. Release 3, December 2005.

[40] ICAO Secretariat: *"Information Paper – Issues of the ICAO Public Key Directory (PKD)"*. April 2006

[41] ICAO: *"Machine Redable Travel Documents; Development of a Logical Data Structure – LDS for Optional Capacity Expansion Technology "*. Revision 1.7, May 2004.

[42] IEEE Computer Society
http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/proceedings/&toc=comp/proceedings/sp/1982/1753/00/1753toc.xml&DOI=10.1109/SP.1982.10011

[43] Agderposten website, article about a man who received his new ePassport with the photo of another, unknown man. 7 May 2006:
http://www.agderposten.no/apps/pbcs.dll/article?AID=/20060508/LOKAL8/105080100&SearchID=73245784568816

Annexes

Annex A – Our e-mail to the Norwegian Security Authority NSM

NB! Only available in Norwegian.

To: postmottak.nsm@mil.no
Subject: Forespørsel masteroppgave om biometriske pass - Til den/ dem det angår

Hei, vi er fire femteårs IKT-mastergradsstudenter ved Høgskolen i Agder, avdeling Grimstad. Vi håper at denne mailen kan sendes til den/dem det måtte angå.

Vi vil i våre hovedoppgaver våren 2006 ta for oss de nye, biometriske passene. Vi er fordelt på to grupper, som har noe forskjellig vinkling på oppgavene. Den ene gruppen fokuserer hovedsaklig på anvendt teknologi, den andre har hovedvekt på standardisering og implementasjon.

Vi har fått beskjed fra vår studieleder, Stein Bergsmark, at det kan være nødvendig å varsle dere om våre oppgaver. Selv om all informasjon vi bruker er offentlig tilgjengelig, har han uttrykt at det kan oppstå bekymring når denne samles og settes i system. Dette kan være fullstendig ubegrunnet, men vi ønsker å være på den sikre siden.

Grunnet mye og uoversiktlig informasjon om biometriske pass ønsker vi også kontakt med en organisasjon eller et firma som kan hjelpe oss. I den forbindelse lurte vi på om dere kunne være til hjelp, enten ved å være kontakt selv eller peke ut noen som kan hjelpe.

Vedlagt er våre to proposals, som forklarer i mer detalj hva våre oppgaver går ut på. Vi håper på snarlig positiv tilbakemelding.

Med vennlig hilsen
Ingvar Narvestad
Mona Forsbakk
Linda W. Olsen
Eili Bjelkåsen

Annex B – Basic Key Generation Algorithms for Ciphers used for Digital Signatures in ePassports

(copied from www.Wikipedia.org.)

RSA

1. Choose two large prime numbers p and q such that $p \neq q$, randomly and independently of each other.
2. Compute $n = pq$.
3. Compute the totient $\phi(n) = (p-1)(q-1)$.
4. Choose an integer *e* such that $1 < e < \phi(n)$ which is coprime to $\phi(n)$.
5. Compute *d* such that $de \equiv 1 \pmod{\phi(n)}$.

The **public key** consists of

- *n*, the modulus, and
- *e*, the public exponent (sometimes *encryption exponent*).

The **private key** consists of

- *n*, the modulus, which is public and appears in the public key, and
- *d*, the private exponent (sometimes *decryption exponent*), which must be kept secret.

DSA

- Choose a 160-bit prime *q*.
- Choose an *L*-bit prime *p*, such that $p=qz+1$ for some integer *z* and such that $512 \leq L \leq 1024$ and *L* is divisible by 64.

  Note: FIPS-186-2, change notice 1 specifies that *L* should **only** assume the value 1024, and the forthcoming FIPS 186-3 (described, e.g., in SP 800-57) uses SHA-224, SHA-256, SHA-384, and SHA-512 as a hash function, *q* of size 224, 256, 384, and 512 bits, with *L* equal to 2048, 3072, 7680, and 15360, respectively.
- Choose *h*, where $1 < h < p - 1$ such that $g = h^z \bmod p > 1$.
- Choose *x* by some random method, where $0 < x < q$.
- Calculate $y = g^x \bmod p$.
- Public key is (p, q, g, y). Private key is *x*.

Note that (p, q, g) can be shared between different users of the system, if desired.

ECDSA

Initially, the curve parameters (q,FR,a,b,G,n,h) must be agreed upon. Also, the entity initiating communication must have a key pair suitable for elliptic curve cryptography, consisting of a private key d_A (a randomly selected integer in the interval [1,n − 1]) and a public key Q_A (where $Q_A = d_A G$).

For the previously mentioned entity to sign a message m, it follows these steps:

1. Calculate e = HASH(m), where HASH is a cryptographic hash function, such as SHA-1.
2. Select a random integer k from [1,n − 1].
3. Calculate $r = x_1 \pmod n$, where $(x_1,y_1) = kG$. If $r = 0$, go back to step 2.
4. Calculate $s = k^{-1}(e + d_A r) \pmod n$. If $s = 0$, go back to step 2.

The signature is the pair (r,s).

Annex C – Our e-mail to the Norwegian Data Inspectorate and their response.

NB! Only available in Norwegian.

To: postkasse@datatilsynet.no
Subject: Elektroniske pass , en mastergradsoppgave - til den/dem dette angår

Hei, vi er to studenter ved Høgskolen i Agder(HiA), fakultet for teknologi i Grimstad. Vi følger masterutdanningen i Informasjons- og Kommunikasjonsteknologi, og skriver i disse dager vår avsluttende masteroppgave. Denne behandler sikkerhets- og personvernproblemer i de nye, biometriske passene. Vi har i den sammenheng lest deres rapport og pålegg fra tilsynet hos politidirektoratet 15.november i fjor, og ønsker å stille et par spørsmål til denne.

Vi håper dere har tid og mulighet til å svare oss, det ville hjelpe vår oppgave. Som gjenytelse kan vi tilby dere å sende vår rapport når den er ferdig etter 29.mai, hvis dette er ønskelig.

Våre spørsmål er:

I rapporten ser det ut som dere godtar at BAC som autentisering er en sikker nok metode. Vi leste i høst en rapport skrevet av Ari Juels(fra RSA laboratories), David Molnar og David Wagner(begge fra UC-Berkely). Rapportens navn er "Security and Privacy Issues in E-passports". I denne nevner forfatterne sin bekymring over at nøklen som brukes til BAC vil kunne være mulig å knekke i løpet av forholdsvis kort tid(få timer) ved hjelp av "brute force" på en vanlig laptop, hvis den er kort nok. Dette er allerede tilfelle i Nederland, som dere sikkert er klar over. Vårt spørsmål er da: Hvordan vet vi at nøklen er lang nok i de 10 årene passet skal fungere, gitt utviklingen i prosessorkraft og annen teknologi?

Senere i rapporten deres nevner dere sjekkrutinene ved utstedelse av pass, og sier at " En sammenlikning av de biometriske data i passbildet med biometriske data i et annet bilde gjøres sikrest maskinelt. En visuell sammenlikning kan medføre feil." Denne linken: http://news.bbc.co.uk/1/hi/technology/3389209.stm er til en artikkel skrevet av BBC. Artiklen inneholder et kort intervju med professor John Daugman ved University of Cambridge, utvikler av algoritmene for iris-gjenkjennelse som UK Passport Service UKPS testet på daværende tidspunkt, og en uttalelse fra Bernard Herdan, chief executive ved UKPS. Professor Daugman uttaler at maskiner er enda dårligere enn mennesker på å gjenkjenne trekk i biometrisk sammenheng. Betyr dette at denne teknologien har hatt en utvikling i det senere som har gjort den bedre egnet enn mennesker?

Har dere også mulighet til å utdype litt mer om hva en risikovurdering innebærer? Hvordan den utføres, hva resultatene kan se ut som osv?

Som tidligere sagt, vi håper dere finner tid og mulighet til å svare på våre spørsmål.

Med vennlig hilsen
Linda Walbeck Olsen og
Eili Bjelkåsen

Svaret kom fra Atle Årnes, senioringeniør ved Tilsyns- og sikkerhetsavdelingen hos datatilsynet:

Til Linda Walbeck Olsen og
Eili Bjelkåsen

Spørsmål 1)
I rapporten ser det ut som dere godtar at BAC som autentisering er en sikker nok metode. Vi leste i høst en rapport skrevet av Ari Juels(fra RSA laboratories), David Molnar og David Wagner(begge fra UC-Berkely). Rapportens navn er "Security and Privacy Issues in E-passports". I denne nevner forfatterne sin bekymring over at nøklen som brukes til BAC vil kunne være mulig å knekke i løpet av forholdsvis kort tid(få timer) ved hjelp av "brute force" på en vanlig laptop, hvis den er kort nok. Dette er allerede tilfelle i Nederland, som dere sikkert er klar over. Vårt spørsmål er da: Hvordan vet vi at nøklen er lang nok i de 10 årene passet skal fungere, gitt utviklingen i prosessorkraft og annen teknologi?

Svar: BAC som autentisering er dårlige greier. Datatilsynet godkjenner ikke løsninger. Det er den behandlingsansvarlige (passmyndighetene) som er ansvarlig for tilstrekkelig sikkerhet. Problemet med BAC er at koden er kjent. Det hjelper ikke med all verdens kode dersom koden er satt sammen av kjente verdier som man kan skaffe fra andre steder. Jeg anbefaler at dere tar en titt på vedlagte uttalelse fra EU's Art 29 gruppe (vedlagt, se punkt 2.4a).

Spørsmål 2)
Senere i rapporten deres nevner dere sjekkrutinene ved utstedelse av pass, og sier at " En sammenlikning av de biometriske data i passbildet med biometriske data i et annet bilde gjøres sikrest maskinelt. En visuell sammenlikning kan medføre feil." Denne linken: http://news.bbc.co.uk/1/hi/technology/3389209.stm er til en artikkel skrevet av BBC. Artiklen inneholder et kort intervju med professor John Daugman ved University of Cambridge, utvikler av algoritmene for iris-gjenkjennelse som UK Passport Service UKPS testet på daværende tidspunkt, og en uttalelse fra Bernard Herdan, chief executive ved UKPS. Professor Daugman uttaler at maskiner er enda dårligere enn mennesker på å gjenkjenne trekk i biometrisk sammenheng. Betyr dette at denne teknologien har hatt en utvikling i det senere som har gjort den bedre egnet enn mennesker?

Svar: Svenske passmyndigheter tar alltid bilde selv av passøkeren. Svenskene benytter et lukket system. I Norge kan passøkeren levere gamle bilder hvor det kun er passøkerstedet som visuelt kontrollerer likhet. I Norge har det allerede skjedd en forveksling på dette punktet som svenskene dermed unngår. Man er i ferd med å implementere det samme system som svenskene har, i Norge. Poenget med med det elektronisk lagrede bildet i passet vil kunne være å benyttebiometrisk sammenlikning. Da må man også kontrollere at dette faktisk er mulig. Et trenet øye kontrollerer ikke biometrien, slikt gjøres "kun" maskinelt.

Spørsmål 3)
Har dere også mulighet til å utdype litt mer om hva en risikovurdering innebærer? Hvordan den utføres, hva resultatene kan se ut som osv?

Svar: I henhold til personopplysningsloven § 13 og personopplysningsforskriften kapittel 2 skal det settes opp en målsetting for informasjonssikkerheten, en strategi, sette opp akseptansekriterier og foreta risikovurderinger. Risikovurderingene vil danne grunnlag for å

bestemme hvilke løsninger man kan implementere og hva slags sikkerhetsnivå som skal settes. Å ha som utgangspunkt at noe er 100% sikkert, er en stor tabbe. Man må klarlegge hvor det svakeste leddet ligger og vurdere tiltak og hvilken usikkerhet man aksepterer og hvordan denne usikkerheten skal håndteres.

Ta gjerne kontakt om dere vil ha fyldigere tilbakemelding.

Med vennlig hilsen

Atle Årnes
Datatilsynet