# Biometric identity verification: A matter of trust

Marck, Everard Johannes van der

*Master thesis*

# Biometric identity verification

A matter of trust

Leiden University – Netherlands
Master Cybersecurity

Marck, E.J. van der (Evert-Jan)
s2816687
30-1-2023

Thesis supervisor: Dr. E. de Busser
Second reader: Dr. Z. Erkin

# Abstract

Transactions with government, either in the physical world or the digital world, can have uncertainty about the outcome and the level of risk, both for the citizen and the public service. Dealing with this uncertainty can be explained with the construct of trust, which is defined as a positive effect on the expected outcome and the acceptance of risk of a transaction in a certain context. Within the context of a transaction with government over the Internet (eGovernment), it shows that identity verification of the citizen can be a cumbersome problem, as no face-to-face verification is readily available. The use of biometric technology might solve this problem, and it is found that for people to trust this technology, and willing to use it, the trust factors of usability, security, privacy and reputation are the main constructs to implement. Within the European Union (EU), biometric identity verification is possible with the European ID-card, and with the design of an electronic identification (eID) solution with mobile biometrics it enables EU citizens to use the biometric data of the ID-card in identity verification over the Internet. The proposed solution is subject to a policy analysis, to investigate whether it is compliant to EU policies and if the found trust factors can be implemented to deliver a trustful eID solution. The analysis shows that the proposed solution is highly compliant and also ensures various trust aspects of biometric technology, mainly usability, security and privacy. The trust aspect of reputation is found to be more likely an aspect of the organisation implementing the whole solution and for eID solutions in particular, the eIDAS Regulation is built upon the construct of reputation. The question arises whether in this way the eIDAS Regulation enhances trust in eID solutions in an effective way. In the analysis of the GDPR the question is raised whether the storage and usage of the biometric data is compliant and in which way could explicit user consent bypass the objections of processing these data. Another complicating factor that is found is that all implementation is done at the Member State level, which makes that the research should be iterated for each Member State. Despite these problems, the findings of this research can be used to enhance the discussion about the implementation of biometric identity verification in the digital world. The constructs of usability, security, privacy and reputation can be used as guidance to deliver a trustworthy eID solution with mobile biometrics and with it ensure trust in transactions with eGovernment.

# Contents

## 1. Introduction

Citizens often have to use public services offered by their governments to form part of society. These services are required for administration of the government, paying taxes, receiving social benefits, healthcare or other public commodities. The interaction between citizens and public services can be seen as a transaction between these two parties.

The last few decades society has become more and more a digital world, where citizens use the Internet for communication and all kinds of transactions that formerly took place in the physical world. Also public services have become available in an electronic way, or, where the nature of the benefits is still in the physical world, at least the administration of the public services has become electronically available and citizens are offered electronic transactions to apply for, verify and change the public benefits.

In all transactions, no matter if they take place in the physical world or the digital world, a successful outcome of the transaction is beneficious to both parties. This also applies to transactions between citizens and public services: it is important that the citizen can rely on the public service to offer the correct and lawful benefits, and that the public service can rely on the citizen to be the intended beneficiary and not to abuse the benefits offered. But the exact outcome of the transaction is not really known in advance and there is always some kind of risk that the transaction goes wrong. Both parties have to manage this uncertainty if they want to go through with the transaction. Dealing with this uncertainty is also called trust (Berg, van den & Keymolen [2017]).

Within the transaction, the public service wants to verify the citizen to be the intended beneficiary and has to do this with all its citizens. Managing the identities of all its citizens has become a major task of governments, and trustful identity verification an important public service (Collings [2008]). In the digital world the problem of identity verification is even bigger, as no face-to-face verification is readily available over the Internet.

This research tries to give a trustful solution for identity verification over the Internet, that can be used for transactions with government. First the construct of trust is being investigated, and how it applies to transactions with government and identity verification (chapter 2). Then a possible solution is presented and it is investigated how this solution could be implemented, making use of the construct of trust (chapter 3). The investigation is performed by a policy analysis within the scope of the EU (chapter 4). The outcomes of the investigation are being discussed (chapter 5) and some conclusions are made (chapter 6).

## 2. Trust in transactions with government

### 2.1 What is trust?

Before investigating how trust works in transactions with government, it should be studied what trust actually is. Many definitions can be found, which has made Berg, van den & Keymolen [2017] come to an analysis of what trust involves: two parties, a trustor (who gives trust) and a trustee (who receives trust), interact in a specific *context* where the *outcome* of the interaction is *uncertain*. The context may vary the expectations of the involved parties towards the outcome, and the uncertainty of the outcome itself makes the interaction have a degree of risk. Trust in the interaction thus "is about holding positive expectations about the outcome without too much control over the course of action" and "therefore, is not about diminishing uncertainty, but about accepting it" (Berg, van den & Keymolen [2017]). For trust to thrive, these concepts of *expected outcome* and *risk acceptance* are very important.

From this analysis it could be understood that trust is only something between persons, *interpersonal trust*. However, Berg, van den & Keymolen [2017] continue by mentioning that trust can also be placed in systems, called *system trust*, and, since the uprise of the use of Internet, there is also a form of trust in and on the Internet, called *e-trust* (Berg, van den & Keymolen [2017]). These other forms of trust, in and through (technological) systems, where the Internet could be considered as a system, can lead to the conclusion that interpersonal trust is nearly impossible with systems. However, it shows that trust in general, by its *context* on the Internet or with systems, can still be looked at in a similar way, and is called *technology trust* (Lankton & McKnight [2011]).

This review of what trust is, is used to come to a working definition for this research. By combining the concepts found, the following definition can be formulated:

> Trust is a positive effect on the *expected outcome* and the *acceptance of risk* in an interaction that has a specific *context*, which can be an *interpersonal* or *technological* context.

From this definition it is seen that trust is something positive, and it also shows that the opposite, distrust, or lack of trust, is a negative effect within the same scope. Another important word in this definition is "effect": trust is something dynamic. This makes it important to investigate also how trust is enhanced, how it can be made more positive, or so to say, how the interaction can be made more trustworthy.

By Das & Teng [2001] it has been investigated that trust is enhanced by either *control* over the outcome of the process or by the reduction of *perceived risk*. This perceived risk is different than actual, calculated risk of one outcome, because of the variance in the many possible outcomes (Das & Teng [2001]). Also mathematically it shows that trust is enhanced by producing better outcomes or by reducing perceived risk (Casadesus-Masanell [2004]).

Looking back at the working definition of trust, the *control* and *perceived risk* still depend on the *context*. In the interpersonal context the control and perceived risk would be about persons and in the technological context the control and perceived risk would be about technology. Again it could be considered that control and perceived risk are only aspects of interpersonal interactions. However, even with or through interactions with (technological) systems, developing enhancements of trust is still possible, by using trust solutions (Berg, van den & Keymolen [2017]).

Another aspect of trust that is mentioned by Berg, van den & Keymolen [2017] is the aspect of interventions by governments, regulators and policy-makers. By developing regulatory mechanisms, countries try to improve control and perceived risk, and thus enhance trust. At first these regulatory

mechanisms were developed as “techno-regulation”, focussing on control over the expected outcome and reducing the security risk. This leads to high levels of compliance, but it made governments in many countries struggle because of the limiting effects on innovation and actual usage (Berg, van den & Keymolen [2017]). Berg, van den & Keymolen [2017] come to the conclusion that governments should consider other regulatory strategies, foremostly by enhancing trust.

Now that it has been explained what trust is and how it is enhanced, it can be investigated how trust works in transactions with government.

## 2.2 Transactions with government

Transactions with government take place between citizens and public services. Successful transactions are very important in the functioning of governments and society. A first step in a transaction is to verify the identity of the other party involved: is it really the intended person or institution to have the transaction with. If the identity is not verified in an adequate way, the transaction may be subject to fraud or lead to other negative consequences. This is what makes identity verification a key component in transactions, both in the physical world and the digital world (Collings [2008]).

In the physical world, the verification of the identity of the citizen by a public service is often done with help of a physical identity document that is issued by the government. In the digital world, the identity of the citizen must be verified through the Internet, which can be a cumbersome problem. This problem of electronic identification (eID) has given way to the development of many solutions. These eID solutions mainly have in common that the citizen is given a user identity that represents the citizen’s identity and the electronic transaction should only take place after the correct verification of the user identity.

In Figure 1 the transactions between citizens and public services in both the physical world as the digital world are drawn schematically, including the interaction with the identity document in the physical world, and with the eID solution and user in the digital world. A successful outcome is important in all these interactions as they all work together to make the transaction as a whole successful.

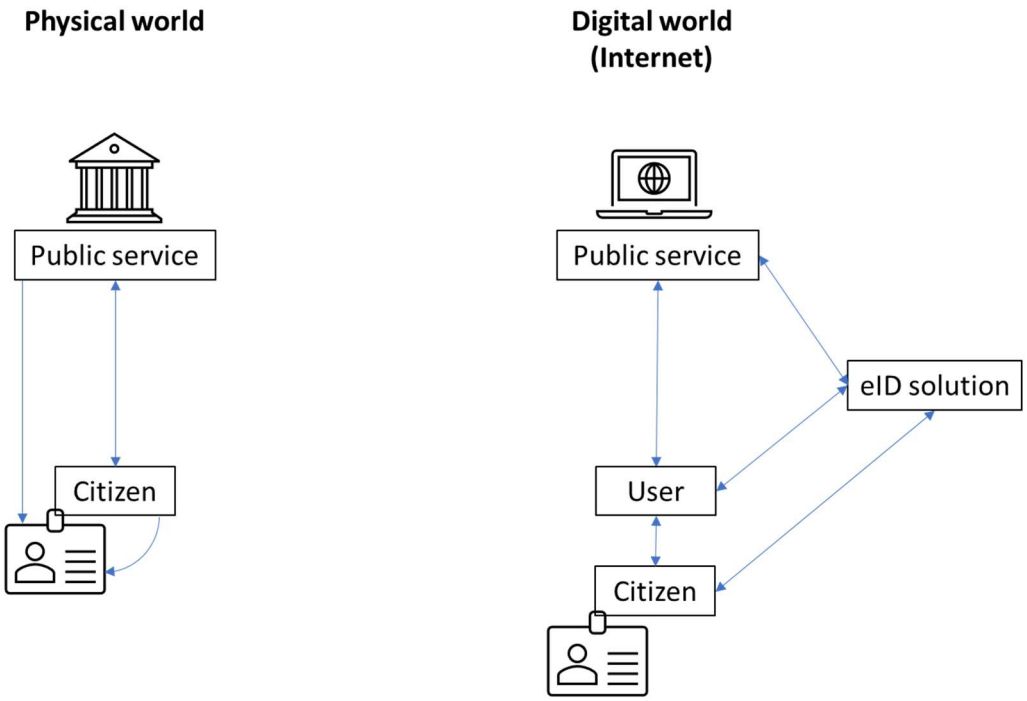



*Figure 1 Interactions in transactions with government*

In the following paragraph, there is explained what the technological developments of identity verification have been and how it evolved in both the physical world and the digital world.

## 2.3 Technological developments of identity verification

In the physical world the verification of someone's identity mostly takes place by verifying an identity document. The ultimate document that declares someone's identity is sometimes called a breeder document, and governments mainly use birth certificates as such evidence of identity. An identity document that is derived from this evidence should be trusted by both the government and the citizen before it is accepted for identity verification (Yang et.al. [2013]).

The history of government issuing identity documents goes a long way back, to medieval times. Before good printing technology was readily available, there were handwritten documents, on paper, just like the breeder document themselves. These documents usually had a textual description of physical characteristics of the person (Caplan et.al. [2001]). When printing of documents came available, mostly printed templates were used, which has the advantage that it is easier to read and contains less casual writing errors. However, usage of the templates was still handwritten by filling in the personal data.

By the time photography was possible, in the 19$^{th}$ century, identity documents started having photographs of the person. Probably the first innovation with this technology was a "photographic ticket", which was invented by William Notman (Hall [1993]). By using a photo of the person, it was not necessary anymore to describe certain aspects of the person, as the photo itself is already a visual description. The technology of photography and of printing was enhanced during the 20$^{th}$ century, and eventually printing on plastic (cards) instead of paper was possible, making way to small

sized ID-cards (Thomas [1995]). These ID-cards were easier to carry around by a person and were less vulnerable to wear and tear.

In the meantime another method of identity verification was developed. Also in the 19th century, the method of fingerprinting was developed by Herschel for the use on official documents (Maguire [2009]). Fingerprints may look like a photograph of the skin pattern on the fingers of a person, but it was shown that not one person has exactly the same pattern as another, not even identical twins, and fingerprints are not subject to aging of the person and sudden changes in looks, two aspects of normal photos. The method of fingerprinting was further developed in the 20th century (Datta et.al. [2001]) and has led to many other uses of this technology. Eventually it became possible to use fingerprints for access to digital systems (Isobe [2001]).

Another development for ID-cards was the possibility of storing digital information on the card. Firstly a magnetic stripe on the card was used but soon it was discovered that using a chip on the card would be better (Krivachy [1985]). Since the contacts of the chip on the card could still be manipulated in a certain way, the use of contactless chips was developed (Abrial et.al. [2001]). By the beginning of the 21st century, all technology came together and made it possible to use *electronic ID-cards with fingerprints* for access to digital systems (Rao et.al. [2008]).

In the digital world the verification of identity mostly takes place by verifying a user identity, as has been shown in Figure 1. This user identity has been issued during the enrolment process, after which the user identity is used for verification in electronic transactions. This two phase process of enrolment and usage resembles the physical world identity verification, but there are also significant differences, which come from the context that is available in the process (Camp [2004]).

An important observation that Camp [2004] makes, is that, with the large history of identity documents and verification in the physical world, the definitions of identity and related terms have changed drastically in the digital world. Also new terms came available as there were no good equivalents in the physical world. The most important change to mention is that the “verification of a user identity” is often called “authentication”, a term broadly used in the context of the Internet.

The history of authentication goes back to the beginning of the computer era in the 1960’s. Ometov et.al. [2018] give a good overview of the evolution of authentication. At first only a username and password were used, which should only be *known to the user*. It soon gave way to several attacks by eavesdropping or guessing the password. By using more complex passwords, this method of authentication was enhanced but soon it was superseded by two-factor authentication (2FA), adding something that is *owned by the user*, such as a token, smartcard or phone. The advantage of using these two factors was that if one of the factors is compromised (lost or stolen), the other factor supposedly remains intact. However, these factors are still transferable, voluntarily to someone else or adversely to an attacker, which has led to the usage of another factor being a characteristic *intrinsic to the user*, such as a behavioural pattern or biometric data. These three factors can nowadays be used for user authentication and is also referred to as multi-factor authentication (MFA).

The use of the Internet changed in the 21st century when mobile devices with advanced functionality came available. These *smartphones* are used with sensitive data, applications and transactions and therefore the need for stronger user authentication on the device has increased. By integrating cameras and other sensors into the device, the use of *mobile biometrics* has become available to a broad public and is nowadays a highly accepted way of verification of the user identity (Rattani et.al. [2019]).

Overall it shows that, both in the physical world and digital world, biometrics (or biometric data) are used in the process of verification of identities. Throughout the centuries, a lot of developments changed the technology used with biometrics. Eventually it can be concluded that "biometrics may be the technology of choice to deliver superior online trust by being the mechanism that best replicates face-to-face exchanges in the technology infrastructure" (Kleist [2007]).

## 2.4 Acceptance of and trust in biometrics

Technology has changed throughout the centuries, changing the way how identities are verified and how biometric data are being used, both in the physical and digital world. This development, shown in the previous paragraph, seems to be accepted by citizens around the world, as it is being used in many identity verification processes (Jain et.al. [2000]).

Acceptance of technology has been investigated in many researches since Davis, in 1986, published his Technology Acceptance Model (TAM), and many adaptations have been developed since then (Lee et.al. [2003]). The main principles of the TAM, perceived usefulness and perceived ease-of-use, can be connected to the more general construct of perceived usability as has been shown by Lah et.al. [2020].

Not only usability is of importance for acceptance of eID solutions, as Tsap et.al. [2019] have investigated in a literature review. Many other factors are found of which some are related to the TAM and its adaptations. It is interesting to see that also trust is found as an acceptance factor, even as the most common category, leading to the notion that "trust is interrelated to most of the other categories and could be divided into subcategories" (Tsap et.al. [2019]). Trust can be seen as a key factor in the acceptance of biometric technologies and it should be made possible to measure trust in an objective way (Kanak & Sogukpinar [2017]).

Kanak & Sogukpinar [2017] then continue by posing that in biometric technology exists a compromise between privacy and security, and both factors mutually influence trust. Eventually, by adding confidence and willingness as factors, it is stated that trust in biometric technology only works if "the privacy is preserved, security is guaranteed, and confidence in the technology as well as public willingness to adopt the technology are all met". These four factors are modelled into a function of trust, which in its turn is an input factor for the traditional TAM, leading to a specially adapted TAM for "Biometric Authentication Systems" called BioTAM (Kanak & Sogukpinar [2017]).

The BioTAM is a highly mathematical model, making it suitable for quantitative research. In this research, a more qualitative approach is pursued. The construct of usability of the TAM and the added constructs of security and privacy, however, are already useful as a starting point. There was a workshop on "Usability, Security, and Privacy of Information Technology" (National Research Council [2010]), which has been rather theoretical, but subsequent studies include usability, security and privacy into a more practical application (Al Abdulwahid et.al. [2015], Alshamari [2016] and Preuveneers et.al. [2021]). An earlier work (Casaló [2007]) already adds the construct of reputation, linking it to, but not combining it with, usability. This approach is tried here as well, applicating the factors of usability, security, privacy and reputation to the concept of trust in biometrics.

Before analysing each of the four factors, a look back is taken at the definition of trust that was formulated in paragraph 1. There trust is defined as an effect on two different aspects of an interaction: the *expected outcome* and the *acceptance of risk*. The factors of usability and reputation are linked to the expected outcome: usability has a relation with the perceived outcome of the interaction that is about to take place, whereas reputation is the perceived outcome regarding the

history of interactions within the same context (Casaló [2007]). The factors of security and privacy are seen as two variables in the construct of acceptance of risk, being perceived security and perceived privacy in the handling of private data (ibid.). All four factors can be drawn in a diagram with relations between them, which has been done in Figure 2. With this diagram in mind, the influence of the factors on trust and the relations between them can be explained.

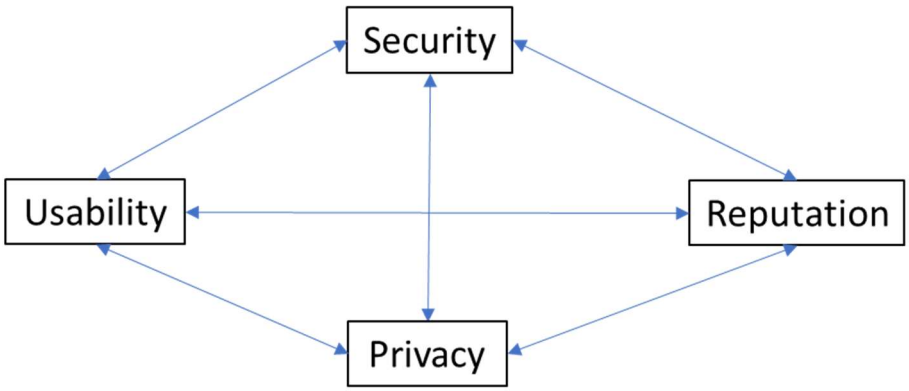



*Figure 2 Factors of trust and their relations*

*Usability*

As seen with the TAM and its adaptations, usability can be seen as a construct of usefulness and ease-of-use of technology. Biometric technology, when used for identity verification, is useful to get better assurance about the identity of a person in a transaction. The ease-of-use of biometrics depends on the specific technology used, as has been seen by Jain et.al. [2000] and Kleist [2007]. Another aspect of the usability of biometrics is the (physical) ability of a person to use the technology. This aspect of usability is mentioned by Schouten & Salah [2008] as a temporal situation that can be handled under the factor of service quality. Oostveen & Lehtonen [2017] studied disability as a permanent situation and call this aspect accessibility, and link it also to inclusivity. Hoffman et.al. [2006] place availability as a separate factor of trust, but Tarafdar [2005] came to the conclusion that availability does influence usability in a positive way. Usability in general, with all its different aspects, has a positive effect on trust (Flavián et.al. [2006]).

*Security*

Traditionally security is seen as a construct of confidentiality, integrity and availability of information (the CIA triad), in which security can be enhanced by the implementation of technical controls (Samonas & Coss [2014]). It is actually this “control” that is also questioned by Berg, van den & Keymolen [2017], urging to look more into aspects of trust. Samonas & Coss [2014] also discuss this aspect, by looking into other, more socio-technical aspects of security, specifically by looking at technical, formal and informal parts of an information system (the TFI model). This leads to other factors like responsibility, ethicality, and correctness, which focus more on integrity of information, an important observation made by Samonas & Coss [2014], who draw the conclusion that the aspects of confidentiality and availability should be researched in a broader context then only security, including privacy as well.

*Privacy*

The concept of privacy is related to personal information or data. Samonas & Coss [2014] show that

the aspect of confidentiality is important for privacy, especially where sensitive personal information is used, and links it also to trust. Jain & Nandakumar [2012] add two more aspects to privacy which are more beyond the technological context: the ownership of personal data and the proportionality of using that data. Prabhakar et.al. [2003] already addressed some other non-technological privacy aspects of biometric data, mentioning the problem of anonymity as a right closely related to privacy, and the problem of revocability which can be seen as the "right to be forgotten". All these, and other, aspects of privacy should not be included as technical controls in the implementation phase of a system, but rather be included as early as possible in the design of a system, leading to the concept of "privacy by design", which enhances trust (Schaar [2010]).

*Reputation*

Reputation has been investigated from many different research areas, especially from economics and marketing (Casaló [2007]), but it can also be seen as a factor of trust, as showed earlier by defining it as "the perceived outcome regarding the history of interactions within the same context". Casaló [2007] further makes a difference between reputation of products, brands, and organisations. Not only this very specific context of one product, brand or organisation influences reputation, also technology in a broader context can influence reputation. Specifically for biometric technology this has been investigated by Feldman [2002], leading to the insight that technology can have the reputation of being a scientific truth: if a technological system identifies a person with biometrics, it must be a reliable result. This can be seen as a positive reputation of biometric technology. There is also negative reputation of biometric technology, which is addressed by Prabhakar et.al. [2003]: some cultures or societies may have rejection of biometric technology because of religious beliefs or because of association with criminal investigation. Another aspect closely related to reputation, investigated by Miltgen et.al. [2013], is innovation. It shows that this is a factor of trust, even when there is no (extensive) history of interactions with the specific technology. This can be seen as lack of reputation, but still being a factor of trust. A final remark about reputation is that the history of interactions within the same context is not necessarily of the same person. In the digital world, on the Internet, there is much information available regarding reviews of products, brands, organisations and technology. The effect of these online reviews has been investigated by Shankar et.al. [2020], which leads to the insight that the mechanism of reputation in the digital world resembles the mechanism of reputation in the physical world.

*Relations between usability, security, privacy and reputation*

All four factors of trust mentioned here are interrelated, and these relations can be investigated further. Alshamari [2016] already performed an extensive investigation of the relations between usability, security and privacy. Several studies found by Alshamari [2016] consider usability as a factor that conflicts with privacy and security, because the primary goal of users in a transaction is not to manage the privacy or security. This notion has led to the development of "usable security", which could lead to less conflict between usability and security (ibid.). Despite the narrow relationship between security and privacy, the development for privacy has been slightly different, focussing on the earlier mentioned "privacy by design" but also looking at privacy policies and offering enhanced privacy settings to the user (ibid.). These developments are more about making "privacy usable" and can be measured by looking at the goals (Johansen & Fischer-Hübner [2019]). An important conclusion to make is that for a technological system to be usable, choices in security and privacy must be made. These choices also affect the reputation. It has already been emphasized that reputation has to do with the expected outcome in a transaction, but it also affects the acceptance of risk and thus has to do with security and privacy. Casaló [2007] has investigated these relations by taking reputation into account, and comes to the conclusion that not only making

choices in security and privacy issues is important, but that it is also necessary to manage the corresponding reputation correctly.

From this whole analysis it shows that trust is influenced by the different factors that are interrelated, specifically for trust in biometrics, and that this trust is important in the acceptance of biometrics. It also gives an insight to the conclusion of Berg, van den & Keymolen [2017] that was referenced in paragraph 1, that governments should develop regulatory strategies for enhancing trust. Governments might do so by developing regulations that make use of these trust factors and the relations between them.

## 3. The use of mobile biometrics in identity verification for eGovernment

### 3.1 Designing eID solutions with mobile biometrics

As seen in the previous chapter, the use of biometrics is important in the verification of identity, both in the physical world as in the digital world. Century-long technology development has changed the way biometrics are used. Governments around the world try to incorporate this technology in their transactions with citizens, to make the transactions have a higher level of trust. This includes online transactions in the digital world, which is often referred to as eGovernment (Scott et.al. [2005]).

In this research, the scope of the European Union (EU) is chosen, which is not a government of one country but of several countries, that are trying to work together to form a transnational society. The foundation of the EU lies within four freedoms: free movement of capital, goods, services and persons, to form an internal market (Oliver & Roth [2004]). Within this internal market and all its transactions, transnational identity verification should be possible: in the physical world by an identity document and in the digital world by an eID solution.

An important EU development in identity verification in the physical world has been the European ID-card that, although developed nationally in all member states, is interoperable and legislated in all EU member states (Szádeczky [2018]). These ID-cards contain biometric information, which brings new challenges and risks for the citizens and the governments, but can also be used as an eID solution for online transactions (ibid.).

Within the European digital world, several eID solutions have been developed, both by governments and private corporations (Arner et.al. [2019]), and these solutions vary between the various EU member states because of differences in traditions and governance (Kitsing [2018]). Therefore, nationally developed eID solutions that are to be used transnationally, should aim at interoperability and try to adjust to sensitive national differences (Andraško [2018]).

Online transactions increasingly take place from mobile devices. Using *mobile biometrics* it may be possible to achieve conventional functionality and robustness of identity verification, while supporting interoperability, mobility, and user experience; bringing greater convenience and enhancing trust for deployment in a broad range of operational environments (Rattani et.al. [2019]). However, designing a mobile biometric system is full of security, privacy, and usability challenges (Gofman et.al. [2019]), and therefore it might be difficult for EU member states to develop trustful eID solutions making use of *mobile biometrics*.

The development of eID solutions has been under investigation by the EU Agency for Cybersecurity (ENISA) and security considerations and recommendations related to the underlying technologies used for eID solutions, among which mobile systems and biometrics, are made (ENISA [2020]). The report also mentions the use of the national ID-cards, and referring to Regulation EU 2019/1157 and International Civil Aviation Organization (ICAO) Document 9303 as standard, the report states: “As all European identity cards shall be compliant, this could be a lever to develop electronic identity schemes and solutions based on these standards […]” and “The Regulation authorises Member States to store data for electronic services such as e-government and e-business in the identity card.” So ENISA [2020] does not question the approach of using a national ID-card as an eID solution.

The use of biometrics is further discussed by ENISA (section B.3 in ENISA [2020]), leading to the insight that security and privacy concerns of fingerprint recognition make that its use is declining in favour of face recognition. Besides, face recognition could be used in the enrolment phase as well as

the authentication phase, by matching the face of the user with the photo stored on the chip of the ID-card.

The ICAO Document 9303 Part 9 [2021] is about "Deployment of Biometric Identification and Electronic Storage of Data" in electronic Machine Readable Travel Documents (eMRTDs). A MRTD is an identity document that contains a machine readable text part known as the Machine Readable Zone (MRZ). The identity of a person (holding an eMRTD) can be verified against the facial image created at the time the identity document was issued. This is done by a match of a current (live) captured biometric image, and the biometric data from the identity document (by using the MRZ to get access to the chip) or from a central database, by creating biometric templates of each (ICAO Document 9303 Part 9 [2021]).

The "facial image created at the time the identity document was issued" is the photo that is used in the enrolment process. ICAO Document 9303 Part 9 [2021] describes that the process is "the capture of a raw biometric sample" and further explains the different possibilities and standards that must be used for it. ICAO Technical Report on "Portrait Quality (Reference Facial Images for MRTD)" [2018] gives a better overview of all possible variations of the process. These variations are shown in Figure 3, which is made according to the ICAO Technical Report Portrait Quality [2018].

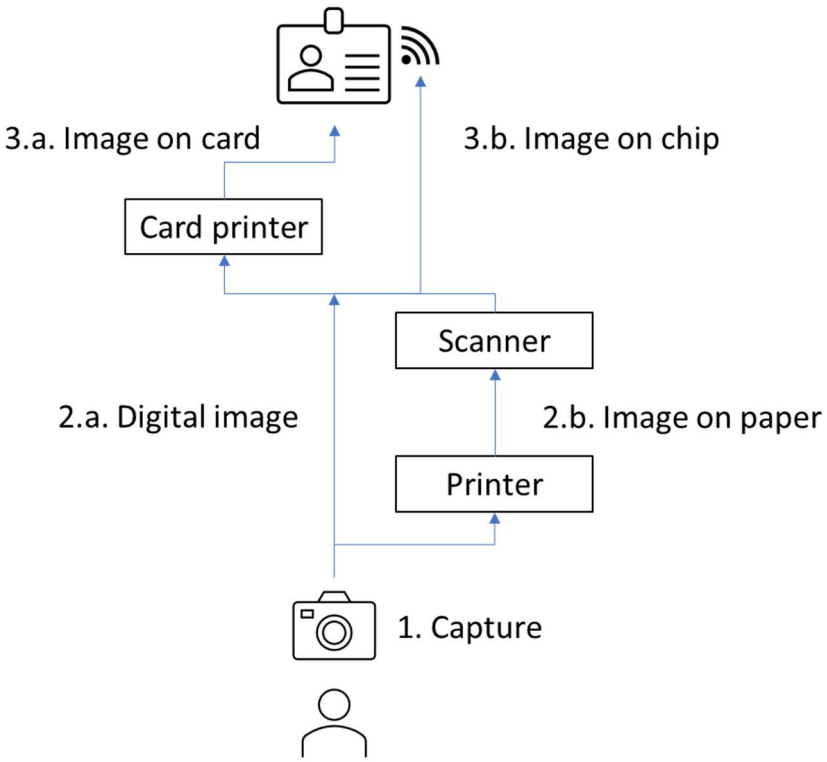



*Figure 3 Enrolment process of a facial image for a national ID-card (according to ICAO Technical Report Portrait Quality [2018])*

The steps necessary for performing the enrolment of the facial image are:

1. A live facial image is captured;
2. The image is either digital (a) or printed on paper (b); the image on paper (b) will be digitalized by a scanner.
3. The image is used by printing it on the card (a) and storing it in the chip (b).

The "match of a current (live) captured biometric image, and the biometric data from the identity document" is the authentication process. With nowadays technology this can be done by using the wireless Near Field Communication (NFC) on a mobile device, extracting the photo from the chip (Geteloma et.al. [2019]) and by using the selfie camera on a mobile device, matching the face of the user (Rattani et.al. [2019]).

In this research, the mobile device is supposed to be owned by the user itself, so the user can choose the device itself and also the Operating System (OS) on it. Probably an app on the device could leverage the technology used for the proposed eID solution. However, the scope of this research is chosen to be only the actual biometric data processing, so regardless of what kind of app, OS or device is being used.

The overall design of the authentication process can be visualized by adding the mobile biometrics technology to the eID solution in Figure 1. The resulting interactions are shown in Figure 4.

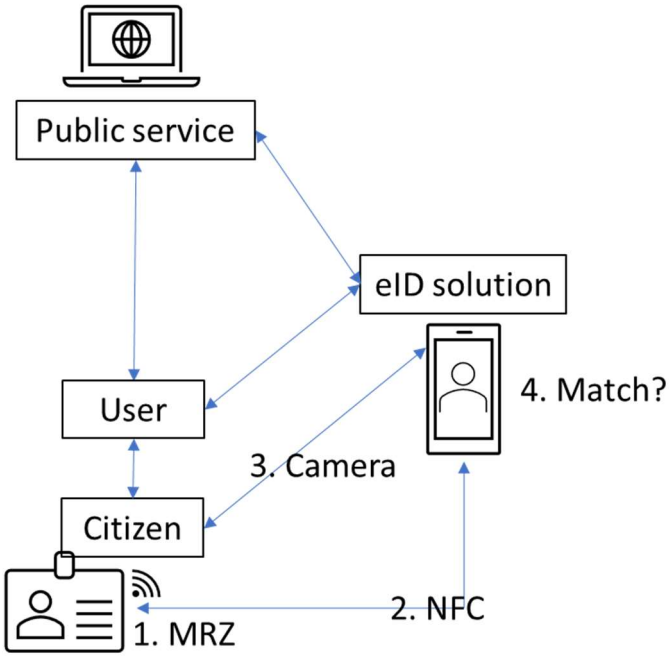



*Figure 4 Authentication process of an eID solution with mobile biometrics*

The steps necessary for performing the identity verification (authentication) are:

1. Read or copy the MRZ from the ID-card;
2. Use NFC with the MRZ to get access to the chip on the ID-card and read the photo;
3. Use the Camera to get a current (live) facial image;
4. Match the photo from the ID-card with the facial image.

Although this design may look promising for use in identity verification for eGovernment, the earlier raised questions about acceptance of and trust in such a solution are not answered yet. In this research, an attempt is made to answer these questions. With the findings from chapter 2 in mind, this is done by looking at the following research question:

How to implement a mobile eID solution using biometric data of the national ID-card that complies with applicable policies within the EU and

that ensures trust in transactions with eGovernment
through the aspects of usability, security, privacy and reputation?

Compliance and trust of the designed solution seems to be a secondary question in this research question. However, if this secondary question is answered *after* designing the solution, it could result in a non-compliant and untrustful solution, making necessary another development iteration. Therefore the question of compliance and trust should be answered *before*, or at least making it *part of* the design.

Therefore the research question is answered by analysing applicable policies within the EU, and looking at the choices that were made (explicitly or implicitly) on the usage of a mobile eID solution using biometric data of the national ID-card. Not only is looked at the scope of using the photo, but also at policies for using the fingerprints, because it might lead to insights that are applicable to the photo or facial image as well. With this policy analysis is not only looked at compliance of the solution but also by acceptance of and trust in the solution. Eventually it can be discussed whether these policies have incorporated the trust acceptance factors and if they ensure trust in transactions with eGovernment.

## 3.2 Analysing applicable EU policies

Before performing the policy analysis, it is necessary to review which EU policies are applicable to national ID-cards, eID solutions and use of biometric data. With the scope of these policies in mind, it then can be determined how the policy analysis can be performed.

The technological developments of identity verification, mentioned in paragraph 2.3, have been used by governments around the world for their ID-cards. Within the EU, member states first implemented EU Regulation No 2252/2004 on standards for security features and biometrics in passports, which relies on the of the International Civil Aviation Organization (ICAO) passport standard Document 9303 (Busch et.al. [2007]). Soon after that, the EU Council was looking to implement those same standards into national identity cards of member states, which has led to a lot of discussion about the usage of the biometric data for ID-cards as well (Wisman [2015]). Eventually it has led to the development of EU-regulation 2019/1157 “on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens”. The ID-cards that come forth of this regulation, need to comply with ICAO Document 9303 (ENISA [2020]). For this research only ICAO Document 9303 Part 9 [2021] is used because of the scope of biometric identification and electronic storage of biometric data.

The EU 2019/1157 references not only ICAO Document 9303, but also other regulations. For the policy analysis in this research a short review is done of all referenced documents and an analysis is made for the scope and only those regulations that are in scope are analysed further. In *Annex 1* this overview is given and for the regulations that are going to be analysed a brief review on their history is done in this section.

Also for eID solutions, technological developments have led to the development of law/legislation. As early as 1999, Finland was the first country to introduce an electronic ID card with identities based on the civil registry and the EU Directive 1999/93/EC on electronic signatures (Rissanen [2010]). It was the starting point for the development of many other national eID solutions with varying success, depending on differences in acceptance factors by citizens (Kubicek & Noack [2012]). Despite these problems, the aspiration of the EU was to use these nationally developed eID solutions in a

transnational context. This has led to the eIDAS framework, which purpose was to enable EU citizens to do cross-border interaction with their own national eID solution (Andraško [2017]), specifically EU-regulation 910/2014 "on electronic identification and trust services for electronic transactions in the internal market".

In addition to this regulation, the ENISA [2020] report mentions that the "Commission Implementing Regulation (EU) 2015/1502 […] details the technical specifications and procedures for each level of assurance for electronic identification" and that therefore compliance with a given Level of Assurance (LoA) for an eID solution is required. To assure that this aspect of compliance with the LoA's is met, the EU 2015/1502 is added to the list of applicable law/legislation for this research.

Not only technology changed and has led to new law/legislation, also the perception on the use of personal data and privacy changed. The right to privacy was already addressed in the 19th century, referring to a more physical "right to be let alone" (Warren & Brandeis [1890]). Since then, the United States (US) had a constant development in privacy law, which extended into the information age of the 20th century (Kramer [1989]). At the beginning of the 21st century, specifically the events on 11th September 2001 have led to a more international emphasis of US law, including privacy law (Solove [2016]). This global change has forced the EU to also become an international player in the protection of privacy of its citizens, and eventually developed the General Data Protection Regulation (GDPR) (Schwartz [2019]), which is EU-regulation 2016/679 "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data". The GDPR is one of the first regulations that specifically mentions biometrics as a special category of personal data and relates it to the process of uniquely identifying persons (Figarella [2017]).

All regulations or standards within the scope of this research that are going to be analysed are summarized in Table 1.

*Table 1 Applicable EU law/legislation*

| Reference | Date | Common name | Working area |
|---|---|---|---|
| EU 2019/1157 | 20 June 2019 | ID-card | Strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement |
| ICAO Document 9303 Part 9 | 2021 | ICAO | Deployment of Biometric Identification and Electronic Storage of Data in MRTDs |
| EU 910/2014 | 23 July 2014 | eIDAS | Electronic identification and trust services for electronic transactions in the internal market |
| EU 2015/1502 | 8 September 2015 | LoA's | Minimum technical specifications and procedures for assurance levels for electronic identification |
| EU 2016/679 | 27 April 2016 | GDPR | Protection of natural persons with regard to the processing of personal data and on the free movement of such data |

Now that the scope of the policy analysis is set, there is looked at how the policy analysis can be accomplished. An important aspect for the implementation of an eID solution is the earlier mentioned two-phase process, the enrolment and the usage (authentication). This should be kept in mind during this whole research, by performing the research for both phases explicitly.

A first aspect to look at is the definition of biometrics or biometric data that is being used in the different regulations. The definitions are then compared to each other and also compared to the applicability on the two phases enrolment and usage of the eID solution.

Then all regulations are analysed for stipulations that can be applied to the mobile usage of biometric data on the national ID-card, again in the phases enrolment and usage. For all stipulations found, an analysis is made of the choices that were made (explicitly or implicitly) and how these choices affect compliance of or trust in the designed solution.

Compliance of a solution is a rather typical yes-or-no question, possibly with an explanation. Since the research question is to have a compliant solution, in the policy analysis it is analysed how the proposed solution can be implemented to be compliant, leading to a probable "yes" as much as possible.

Trust in a solution, as seen in chapter 2, "is influenced by the different factors that are interrelated, specifically for trust in biometrics, and that this trust is important in the acceptance of biometrics". This influence on trust can be positive (enhancing trust) or negative (diminishing trust). In this research a qualitative approach is chosen, by analysing (possible) positive and negative effects on the aspects of trust of the proposed solution.

To produce comparable results, a special template is used for the policy analysis, in which all mentioned aspects are addressed. The template is shown in Table 2.

*Table 2 Template for qualitative policy analysis*

| **#** **Policy:** (reference) | **Reference:** (textual reference) | |
|---|---|---|
| **Applicable to:** | **enrolment** | **authentication** |
| **Compliance:** | Analysis of how the solution can be compliant *or* Not applicable | Analysis of how the solution can be compliant *or* Not applicable |
| **Trust factor Usability:** | Analysis of positive/negative effects on trust *or* Not applicable | Analysis of positive/negative effects on trust *or* Not applicable |
| **Trust factor Security:** | Analysis of positive/negative effects on trust *or* Not applicable | Analysis of positive/negative effects on trust *or* Not applicable |
| **Trust factor Privacy:** | Analysis of positive/negative effects on trust *or* Not applicable | Analysis of positive/negative effects on trust *or* Not applicable |
| **Trust factor Reputation:** | Analysis of positive/negative effects on trust *or* Not applicable | Analysis of positive/negative effects on trust *or* Not applicable |

After performing this qualitative policy analysis, a quantitative analysis on the results is done. This is done by counting the number of applicable elements that were analysed for each policy, and counting if these elements can be used for ensuring trust aspects. This can show to what extent the policies can be used to ensure trust. The resulting numbers will be shown in the template of Table 3.

*Table 3 Template for quantitative analysis of the results*

| Policy | Total analysed elements | Number of analysed applicable elements for enrolment | | | | | Number of analysed applicable elements for authentication | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Compliance | Usability | Security | Privacy | Reputation | Compliance | Usability | Security | Privacy | Reputation |
| **ID-card** | | | | | | | | | | | |
| **ICAO** | | | | | | | | | | | |
| **eIDAS** | | | | | | | | | | | |
| **LoA's** | | | | | | | | | | | |
| **GDPR** | | | | | | | | | | | |

Chapter 4 contains the whole policy analysis, after which a general discussion on this research is done in chapter 5.

## 4. Policy analysis: implementing a mobile eID solution using biometric data of the national ID-card

### 4.1 Definitions of biometric data

Before analysing the policies as a whole, a specific analysis of the definition of biometric data is done. Each policy has been developed for its own working area (see Table 1) and differences in the use of biometric data are to be expected. A search in the policies is done on the use of the word "biometric". In Table 4 the found definitions in the different policies are listed.

*Table 4 Definitions of biometric data / biometrics*

| Reference | Common name | Definition of biometric data / biometrics |
|---|---|---|
| EU 2019/1157 | ID-card | Mentions biometric identifiers and biometric data.<br>Uses 'biometric data' for a facial image of the holder of the card and two fingerprints in interoperable digital formats. |
| ICAO Document 9303 Part 9 | ICAO | Mentions that 'biometric identification' is a generic term used to describe automated means of recognising a living person through the measurement of distinguishing physiological or behavioural traits. |
| EU 910/2014 | eIDAS | None, but mentions "personal data" and refers to the GDPR.<br>'person identification data' means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established. |
| EU 2015/1502 | LoA's | 'inherent authentication factor' means an authentication factor that is based on a physical attribute of a natural person, and of which the subject is required to demonstrate that they have that physical attribute. |
| EU 2016/679 | GDPR | 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. |

From these definitions it can be seen that only the GDPR has a proper definition of biometric data and mentions not only the physical characteristics of a person, but also the physiological or behavioural characteristics. Although these additional characteristics are out of scope of this research, it shows that the GDPR has a complete scope. The "specific technical processing" refers to some technology being used and the purpose of the processing, to "allow or confirm the unique identification" of a natural person, with the examples of facial images or fingerprints, adheres well to the scope of this research and therefore is used as the preferred definition for the policy analysis in this chapter.

The complete policy analysis is written down in Annex 2. In the remainder of this chapter the most prominent findings are rewritten in separate sections.

### 4.2 Using standards in legislation

The ID-card Regulation, after general articles on the subject matter and scope, starts setting standards for the format, specifications and security in Article 3. The size of the ID-card is set to be

"ID-1" format (ID-card, Article 3, Paragraph 1), without mentioning or referring what is meant by it. A search on the Internet reveals that this format is specified in the international standard ISO/IEC-7810[1], indicating the physical dimensions of the card. It is unclear why the format aspect is not referenced in a proper way.

The MRZ forms another standardized aspect of the ID-card in the same paragraph. However, the reference to the ICAO Document 9303 as a standard is put as "shall be based on" (ID-card, Article 3, Paragraph 1) and "should be taken into account" (ID-card, Preamble 23), which is a vague way of setting a standard and could lead to discussion about compliance to the standard. All ID-cards should be compliant to the regulation, and therefore compliance to ICAO Document 9303 is supposed to be met as well.

Only Part 9 of the ICAO Document 9303 has been put in scope of this policy analysis. Specifically this part was reissued in the eighth edition of 2021, which is after the issuance of the ID-card regulation in 2019. It is unclear whether the ID-card regulation would always pursue compliance to the most recent version of the referenced standards. This is a common problem for using standards in legislation, as standards have their own pace of renewal, independent of legislation.

Looking at the ICAO standard, it is interesting to see that the eMRTD, as a subset of the whole set of MRTDs, must also be conform the whole set of standards in the ICAO Document 9303 (ICAO, Paragraph 2.1). For this policy analysis this is seen as that the ID-cards having an eMRTD shall be compliant to the ICAO standards.

Another aspect that is in the ICAO standard, is that other standards are referenced (ICAO, Chapter 7). It is a "normative" list of references to mainly ISO/IEC standards, of which several standards seem to be within the scope of the ID-card with electronic and biometric data. Supposedly the ID-card is to be compliant to all these standards. It is unclear, however, why certain more general ISO/IEC standards on the use of biometric data, like ISO/IEC 24745 on Biometric information protection[2] and ISO/IEC 30107 on Biometric presentation attack detection[3] do not form part of the normative references.

Although the ICAO might not be a well-known organisation for providing standards on identity documents in general and eMRTDs in specific, many people around the world use these standardized identity documents for travelling. Many people put their trust in the identity documents without knowing the exact details of the standardisation. It seems that the reputation of the identity documents issued by EU Member states is positive and this reputation is made explicit in the EU regulation for ID-cards. The implicit trust in ICAO is also forwarded to the ISO organisation and its standards, although the traveller might not know about all of these aspects (ID-card, Article 3). It seems to be that, in general, standards have a good reputation, and therefore people put their trust in them.

Another more general aspect of standards that is found in the analysis, is about usability. The ICAO standard is full of usability aspects, mentioning explicitly the aspects of interoperability, uniformity, reliability, practicality and durability (ICAO, Paragraph 3.2) as key considerations for biometric applications with eMRTDs. Although this sounds promising, it is unclear whether the standards really look into usability for all people, for example disabled people, which is the aspect of inclusivity. Maybe the standards are only usable for "standard" people.

[1] See https://www.iso.org/standard/70483.html (accessed 27-1-2023)
[2] See https://www.iso.org/standard/75302.html (accessed 27-1-2023)
[3] See https://www.iso.org/standard/53227.html (accessed 27-1-2023)

The LoA's can also be seen as a standard, as they contain practical implementation guidelines for eID solutions. It also references the standard ISO/IEC 29115 on a framework for managing entity authentication assurance[4] (LoA's, Preamble 3), but explicitly chooses to differ from the standard. Another aspect that is referenced, but indirectly, is the "attack potential" (LoA's, Annex, Paragraph 2.2.1. and 2.3.1), determined by the Common Criteria (CC) as part of their standard and evaluation methodology[5]. It is unclear why the CC standard and evaluation methodology is not referenced in a proper way nor even mentioned in the preambles. It seems that the eIDAS regulation and its LoA's has been developed differently compared to the ID-card regulation, adhering less to commonly accepted standards.

In general it shows from the policy analysis that standards form an important input to the EU regulations. These standards contain many implementation aspects to be considered for the proposed solution.

### 4.3 Collection of biometric identifiers and dignity of the person

One of the purposes of the enrolment process is the collection of biometric identifiers that later are used in the authentication process. The ID-card Regulation gives special attention to persons who are not able to give their biometric identifiers (ID-card, Preamble 27), mentioning the dignity of the person as the main concern. This dignity is then explained as the need for having "specific considerations relating to gender, and to the specific needs of children and of vulnerable persons".

Later on in the regulation, only the exemption to give fingerprints is mentioned (ID-card, Article 3, Paragraph 7), for children and for persons who are physically not able to give fingerprints. There is no explicit mentioning of other biometric identifiers, as the facial image, and possible exemption, nor for other vulnerable persons. It seems that no thought is given to situations where, maybe temporarily, it is not possible to collect a proper facial image and what is does with the dignity of the person, like for example with very small babies or people with disabilities in the eyes. Also religious beliefs about facial images or necessary religious items in the facial image might lead to discussion about dignity.

The (temporal) impossibility of taking fingerprints is also linked to the validity period of the ID-card and also other exceptions in validity for "persons in special and limited circumstances" are mentioned (ID-card, Article 4, Paragraph 1-3). Again, no specific attention is given to the facial image, which may lead to discussion for certain people.

The dignity of the person with respect to the collection of biometric identifiers is then put in a broader context, mentioning Human Rights and other international conventions (ID-card, Article 10, Paragraph 2). Member States (of the EU) should have appropriate procedures in place that respect the dignity of the person. This makes dignity an aspect of the reputation of the procedures and the Member State involved. The procedures and hence the Member State can have a good or bad reputation for respecting the dignity of the person.

[4] See https://www.iso.org/standard/45138.html (accessed 27-1-2023)
[5] See https://www.commoncriteriaportal.org/cc (accessed 27-1-2023)

### 4.4 Qualified and duly authorised staff

The procedures for collecting biometric identifiers shall be operated by "qualified and duly authorised staff designated by the authorities responsible" for issuing the ID-cards (ID-card, Article 10, Paragraph 1). It is left open by the regulation how staff should be qualified and duly authorised and how a citizen can be aware of the qualification and authorisation. In the physical world the authorisation is mostly accomplished just by seeing the clerk or officer behind the desk with all the necessary equipment for the enrolment process. The qualification of the clerk or officer however is more difficult to determine by the citizen. If the whole procedure goes well and smooth, the qualification is perceivable, but if mistakes are made in the procedures of the enrolment process, the qualification of the clerk or officer could be discussed. Then also former experiences of the citizen with the enrolment process, possibly with other clerks or officers or at a different issuing authority, come into account, making it a reputation aspect.

Once the data is in the chip on the ID-card, using the biometric data is limited to "duly authorised staff of competent national authorities and Union agencies" (ID-card, Article 11, Paragraph 6). Taking this literally, this would mean that only a person could use the biometric data, and not a machine or technology. However, any technical solution, which could be seen as a procedure that involves technology, should only be *operated by* duly authorised staff. In physical identity verification this usually is compliant when staff like a border patrol or police officer does the verification with some device the officer operates. In digital identity verification the whole procedure is through/over the Internet, and without a person on the other side, only a machine, so compliance is only possible if the solution acts *on behalf of* duly authorised staff. This compliance could be discussed. An additional discussion could be raised if *supervision by* duly authorised staff should also be necessary, which might be problematic in the digital world with the proposed solution with mobile biometrics operated by the citizen themself. Finally, the question could be raised whether the citizen themself has the authorisation to use the biometric data. Such authorisation does not come from this regulation, so it would make the whole proposed solution in this research discussible.

Also the ICAO standard addresses the usage of the biometric data by stating that "the issuing State or organization may require that the data cannot be accessed except by an authorised person or organization" (ICAO, Paragraph 5.3), referring to privacy law or practice. To limit the access, the ICAO standard offers encryption techniques, which is a technical measure that can be implemented. Here the discussion could be whether the EU Member States are free to choose which data are to be protected from usage, as the ICAO standard nor the ID-card regulation seem to give a proper decision about it.

### 4.5 Technical implementation aspects

Besides references to standards, there are also many technical implementation aspects that are addressed directly in the different EU-regulations, starting with the ID-card itself. The already mentioned format of the card is to be ID-1 (ID-card, Article 3, Paragraph 1), which is also used for banking cards and therefore also known as "credit card size". The usability of this card size is well-known to most citizens as most people use banking cards in their daily lives. Using this format for the identity card therefore has a positive effect on usability. However, being a smaller format than a passport for example, some people might have (negative) usability issues because of easy misplacement or loss of the card, which could cause problems with the security and privacy of the card.

Another aspect of the card itself, is the Machine Readable Zone (MRZ) on the card (ID-card, Article 3, Paragraph 1), which is needed to get access to the storage medium. In its name is already a "negative" aspect of usability, because it says that it is "machine readable", so it is likely that a citizen would think that it is not human readable. However, the MRZ is just a few lines of text printed in an special Optical Character Recognition (OCR) font. With OCR technology (used with a photo camera or other scanning device) it is possible to have the device "read" (recognize) the characters and process them further. In the MRZ some main data elements of the identity card are present (as specified in ICAO Document 9303 part 11), among which the document number, the birth date and the expiry date. These three data elements are exactly the only ones needed to get access to the storage medium (electronic chip access by BAC or PACE as specified in ICAO Document 9303 part 11), something that is not known to most people using eMRTDs. So instead of scanning the MRZ with a camera, it is also possible to use the three data elements by typing them in manually, which could have a positive usability effect on citizens. In ICAO document 9303 there is mentioned another method of access to the storage medium, by the Card Access Number, which is a 6-digit number: "In contrast to the MRZ (Document Number, Date of Birth, Data of Expiry) the CAN has the advantage that it can easily be typed in manually." So in the ICAO document there is thought about usability.

The whole ICAO Document 9303 part 11 is about "Security Mechanisms for MRTDs", so security seems an important aspect as well. However, the aspect of security of the MRZ is not mentioned explicitly in this paragraph of the EU-regulation on ID-cards. A citizen could think that the MRZ is not very important for the security of the identity card and be careless about its use. This has a negative effect on the whole security of the card. Attacks on the identity card could be possible, for example by "shoulder-surfing" the MRZ with a camera or just by convincing the citizen that it is no problem to scan the MRZ or give its data away. Subsequently, the attacker could get access to the storage medium as well. Security awareness might be needed to have a positive security effect.

Privacy of the MRZ is similar to the security of it. Many people might not be aware that the MRZ contains exactly the data as shown on the "normal" part of the identity card. So when people make a photocopy of their identity card (for use in identity verification in the physical world), they might not know that the MRZ can still be used to retrieve personal data from the storage medium, that was supposed to be private. Awareness of this issue could have a positive effect.

The storage medium itself is an important technical aspect of the ID-card, which should be "highly secure" (ID-card, Article 3, Paragraph 5). The term "highly secure" is very vague and not defined. Also the reason why it must highly secure is not mentioned in paragraph 5. In paragraph 6 however, the reason is stated: "to guarantee the integrity, the authenticity and the confidentiality of the data". It could be discussed why only these aspects of security are mentioned and not just "security" in general. The privacy aspect is indirectly within the same terms as for security, but not mentioned explicitly.

On the storage medium the biometric identifiers are to be stored (during enrolment) and be accessible (during authentication), and it shall contain "a facial image of the holder of the card and two fingerprints in interoperable digital formats" (ID-card, Article 3, Paragraph 5). For the solution to be able to read the biometric data, specifically the digital format is important, and the format is in the standards that are referenced in the paragraph. The facial image is stored as an image file, and not as a pattern as is done with the fingerprints. This means that the facial image is always displayable in its original format, as a photograph, while the pattern of the fingerprints can only be used to match with a live capture. This difference in usability of the digital format is not mentioned explicitly, nor are its security and privacy consequences.

Although the processes of capturing of biometric identifiers (ID-card, Article 3, Paragraph 5) and the authentication of the storage medium and access and verification of the biometric data (ID-card, Article 3, Paragraph 6) are mentioned, there is no explicit mentioning of the usability, security or privacy aspects of these processes. For these aspects there is a general reference, which eventually shows to be an implicit reference to the ICAO Document 9303 and underlying ISO standards. An aspect of the process which seems to be forgotten is the surroundings of where the enrolment or authentication takes place. The room, or maybe a private booth, where the citizen undergoes the enrolment and authentication process should also be considered for usability, security and privacy aspects.

The biometric identifiers used in the enrolment process, before they are securely stored on the ID-card, should also be stored "in a highly secure manner and only until the date of collection of the document and, in any case, no longer than 90 days from the date of issue" (ID-card, Article 10, Paragraph 3). Again "highly secure" is a very vague term that is used. Although this stipulation is to assure that the biometric data is not used for other purposes, the citizen cannot perceive how the security and privacy of the data is being assured. It leaves no other option than to trust the issuing authority to be compliant.

The ICAO standard gives some more detail to the technical aspects of the eMRTD. The validity period of the document is linked to "the limited durability of documents and the changing appearance of the document holder over time" (ICAO, Paragraph 2.2), which is clearly a usability aspect. Also the link is made with technology evolvement, as security and privacy issues may arise during the lifecycle. This technological change is mentioned again, stating that "implementation of most biometrics technologies is subject to further development" (ICAO, Paragraph 3.5).

In the key considerations for biometric applications for eMRTDs, ICAO further specifies the technical reliability, as "the need to provide guidelines and parameters to ensure issuing States or organizations deploy technologies that have been proven to provide a high level of confidence from an identity confirmation viewpoint; and that States or organizations reading data encoded by other issuing States or organizations can be sure that the data supplied to them are of sufficient quality and integrity to enable accurate verification in their own system" (ICAO, Paragraph 3.2). In the proposed solution this is an important aspect for the facial image that is used for verification. The question is how the proposed solution can assure the quality and integrity of the biometric data during the enrolment process, as it is the issuing authority that is responsible for the process and the used technologies in this process. The same question for the authentication process is easier to answer, as the eID solution itself is responsible. Besides, ICAO gives a solution by "the application and usage of modern encryption techniques, particularly Public Key Infrastructure (PKI) schemes" (ICAO, Paragraph 5.3). These encryption techniques provide signing of the data by the issuing authority and limiting access by the use of certificates, and both mechanisms can be used in the authentication process. Decisions about the use of the encryption techniques however still are to be made by the issuing authority of the ID-card.

The only technical aspect that comes forward In the eIDAS Regulation is that of interoperability. Although the eIDAS aims to be technology neutral, the eID solutions that are to be compliant must be interoperable by the reference of minimum technical requirements. Most of these technical requirements are to be found in the assurance levels (LoA's), but also in other requirements as "common operational security standards" (eIDAS, Article 12, Paragraph 1-4). As not all security standards can be analysed, the analysis of the LoA's for technical aspects is supposed to be sufficient for this research. The LoA's, being an EU regulation itself, uses the enrolment and authentication processes, which correlate to the processes of the proposed solution. The additional process of

"electronic identification means management" is supposed to take place between and during enrolment and authentication and therefore in scope of this analysis (LoA's, Article 1, Paragraph 2).

The first aspect, that can already take place before the enrolment process, is awareness about the terms and conditions and security precautions related to the eID solution (LoA's, Annex, Paragraph 2.1.1). This is mainly a usability aspect than can be negative for trust, as the user might be overwhelmed with all the conditions and might feel unsure about the usage being doable and secure. Privacy precautions are not explicitly mentioned, but can also form part of the awareness, as not only the technology of the eID solution is at stake, but also the processes. Only if the user is confident enough, it will engage into the enrolment process with the biometric data.

The enrolment process of an eID solution is about verifying personal data, mostly against an authoritative source (LoA's, Annex, Paragraph 2.1.2). The whole procedure of enrolment for the ID-card is supposed to be compliant for assurance level High, as the identity verification is done with "photo or biometric identification evidence". A usability aspect that could be discussed is how changes in looks should be assessed and how can be determined whether the match with the photo is sufficient. Normally with eID solutions the match could be performed by a first authentication, but for the ID-card it is not probable that it is available at the moment of enrolment, making it unsure whether the authentication process really can be performed.

The proposed solution makes use of the authentication factor of possession (the ID-card) and the intrinsic factor of the facial image. These are two factors of different categories and the intrinsic factor "can be reliably protected by the person to whom it belongs against use by others" (LoA's, Annex, Paragraph 2.2.1), which is a requirement for assurance level High. There is however another requirement which is harder to accomplish, which is about protection against the duplication of the eID solution. The ID-card itself might be hard to duplicate, as well as the chip that is protected to cloning (by the ICAO standard), but after reading the facial image from the chip, it is readily available for other use, and an electronic image is always a "duplication". For compliance to the LoA's there must be additional safeguards so that a duplicated image cannot be used. The solution for this is to be found in the Chip Authentication that is described in the ICAO standards. So the ID-card being compliant to the ICAO standards is supposed to be compliant to this LoA as well, if, and only if, for each authentication, the chip is to be verified with Chip Authentication.

For the eID solution to be compliant to assurance level high, it must protect "against attackers with high attack potential" (LoA's, Annex, Paragraph 2.2.1 and 2.3.1). There is no proper reference of how this attack potential is to be assessed, although in the section on standards (4.2) it is found to be part of Common Criteria. It remains unclear if the eID solution must be evaluated by the Common Criteria or that other methods may be used. This is left for further research, but the question remains whether the proposed solution could achieve this high attack potential.

After the enrolment process, it is important that the eID solution is delivered "into the possession of the person to whom it belongs" (LoA's, Annex, Paragraph 2.2.2). The ID-card, where the applicant "shall appear in person at least once" (ID-card, Article 10, Paragraph 1) is supposed to be compliant to this assurance level Substantial. To obtain level High an additional stipulation is made, about the activation process. Specifically this could be done via an activation code that is only to be known to the applicant and that is delivered in a secure way, or it could be done with a first authentication to a special "activation service". With this activation process the proposed solution is supposed to be compliant to assurance level High. However, the consequence of this activation process is that there should also be a register for the activation status of the eID solution, and this status is to be checked before each authentication. For the proposed solution it could be possible to have the activation

status on the ID-card itself, so that a centrally (e.g. via Internet) accessible register is not necessary. However this would require an additional implementation on the chip of the ID-card. Further stipulations about the activation process or register are not found, so either solution could be viable.

After the activation, it should be possible for the user to "suspend and/or revoke an electronic identification means in a timely and effective manner", and subsequently, "if the same assurance requirements as established before the suspension or revocation continue to be met", it should be possible to reactivate (LoA's, Annex, Paragraph 2.2.3). These stipulations shed new light to the possible solutions of the activation register. The "electronic identification means" in the proposed solution is the facial image on the chip on the ID-card. So it should be possible to suspend or revoke the usage of the facial image. However the main use of the facial image is the (physical) identity verification with the ID-card, which cannot and should not be suspended or revoked, unless when the ID-card is lost or stolen. Technically it might not be possible to suspend or revoke the usage of the facial image and legally it should not be possible, so therefore the proposed solution should invoke a central register of lost or stolen ID-cards. If this is not possible the suspension or revocation should be accessible in the activation register, which then should be centrally accessible as well. After all, it seems that a centrally accessible activation register, which also serves for suspension and revocation status, is the proper way of implementation.

Finally, if the eID solution is to be replaced or renewed, the proposed solution can only accomplish this by applying for a new ID-card, which follows the whole enrolment process again, with a new facial image. Therefore compliance to the stipulation that with renewal or replacement "the identity data is verified with an authoritative source" (LoA's, Annex, Paragraph 2.2.4), is met.

### 4.6 Reference and compliance to the GDPR

As the biometric data that are being used in the ID-card are personal data, it is logical that the ID-card regulation refers to the GDPR for protection of this data. However, the terms "without prejudice [to the GDPR] Member States shall ensure" the protection of the data are vague and do not stipulate compliance (ID-card, Article 11, Paragraph 1). Subsequently the controller of the data is determined to be "the authorities responsible for issuing identity cards" (ID-card, Article 11, Paragraph 2) and the role of the supervisory authorities (to the GDPR) is determined (ID-card, Article 11, Paragraph 3). Also the liability "in respect of breaches of obligations with regard to personal data" (ID-card, Article 11, Paragraph 4) is mentioned. It is unclear why not a proper reference to the GDPR is made for this whole Article.

An important data protection element that is defined in the ID-card regulation, is the purpose of the biometric data processing. The purpose is determined to be the verification of "the authenticity of the identity card" and "the identity of the holder by means of directly available comparable features where the identity card … is required to be produced by law" (ID-card, Article 11, Paragraph 6). In the physical world this verification is seen with border and police control. In the digital world the proposed solution is accomplishing this by comparing the facial image on the ID-card with a live image, but the question remains whether it is required by law and it would make the proposed solution discussible.

The ICAO standard also refers to privacy law, but in a more direct way by stipulating that the storage of biometric data "shall comply with any national data protection laws or privacy laws of the issuing State or organization" (ICAO, Paragraph 3.5). It is unclear, however, how the ICAO could force compliance through their standards.

The eIDAS regulation refers to the predecessor of the GDPR, supposedly because the GDPR was not available yet when the eIDAS was developed. However, it is understood that the "processing of personal data shall be carried out in accordance with" the GDPR (eIDAS, Article 5). Again a rather vague stipulation is used, that does not enforce compliance in a proper way.

Despite the poor references to the GDPR, for the proposed solution compliance to the GDPR is analysed further. The GDPR considers biometric data as a special category of personal data and its processing "shall be prohibited" (GDPR, Article 9, Paragraph 1). So processing of the facial image for the proposed solution cannot be compliant to this paragraph. Looking at the preamble (51) of the GDPR, there is an additional stipulation about the processing of photographs, which should not be considered of a special category, as "[photographs] are covered by the definition of biometric data *only when* processed through a specific technical means allowing the unique identification or authentication of a natural person". This is the case in the proposed solution, which confirms the conclusion that the processing of the facial image is prohibited.

However, Paragraph 2 of the same Article in the GDPR lists the exemptions on this prohibition and this list is further analysed. A possible exemption could be if the "processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law" (GDPR, Article 9, Paragraph 2 [g]). Processing of the facial image in the enrolment phase, is necessary for the issuing of the ID-card, which can be used to exercise the freedom of movement, as portrayed in the ID-card regulation (EU 2019/1157). This seems a substantial public interest for the exemption to be applicable. In the authentication phase of the proposed solution, processing of the facial image is necessary for the verification of the identity for eGovernment. In the ID-card regulation (EU 2019/1157) this processing is found in Article 11, Paragraph 6. However, that purpose is restricted as discussed in this section, and therefore it is discussible whether identity verification for eGovernment is a substantial public interest. An exemption that might be used for processing the facial image in the authentication phase is when "the data subject has given explicit consent" (GDPR, Article 9, Paragraph 2 [a]). The implementation of such a consent in the authentication process is left for further research.

To complete the Article about the processing of special categories of personal data, the GDPR states that "Member States may maintain or introduce further conditions, including limitations, with regard to the processing of … biometric data" (GDPR, Article 9, Paragraph 3). This means that, for the implementation of the proposed solution in EU Member States, the compliance should be investigated on a Member State level and that the proposed solution could be incompliant in certain Member States. The analysis of compliance on Member State level is left for further research.

### 4.7 Reputation as regulatory aspect

Reputation as trust aspect of technology is hard to find in the analysed regulations. This might be because the technology that is being used (eMRTD and mobile biometrics) is rather innovative or that reputation is not seen as important for the acceptance of the technology. However, reputation of organisations that are involved in the use of the technology, seems to have a more important role in the regulations.

It starts with the trust that is put in the standards (section 4.2). The ID-card Regulation builds upon the reputation of the ICAO, which in its turn builds upon the reputation of the ISO/IEC organisation. Having the issuing authorities of the ID-card, and hence the Member States, responsible for compliance to the standards, and the fact that the citizen has direct contact with the issuing

authorities in the enrolment process, makes that the reputation of the ID-card transfers to the issuing authorities: if something is not compliant in the usability, security or privacy of the ID-card, the issuing authorities are held responsible, changing the reputation of the issuing authorities. It is more likely that the issuing authorities or Member States will be blamed for a bad implementation, than that ICAO or ISO/IEC are blamed for bad standards.

It can also be seen that most technical aspects do not have a direct reputation aspect either (section 4.5). Here also the reputation aspect seems to be transferred to the organisation that is responsible for the compliance to the technical aspect.

Therefore it is interesting to see that the eIDAS Regulation states that it "should be technology-neutral. The legal effects it grants should be achievable by any technical means provided that the requirements of this Regulation are met." (eIDAS, Preambles [27]). The main way how this is accomplished is by the mutual recognition of eID solutions between Member States (eIDAS, Article 6). This mutual recognition is formalized by the publication of the list of recognized eID solutions, which is called notification (eIDAS, Article 9). An important condition for the recognition is that the eID solution "shall specify assurance levels … for electronic identification" (eIDAS, Article 8) and that these assurance levels are met by the issuing party of the eID solution and the notifying Member State (eIDAS, Article 7).

This rather complicated way of putting things is to show that, although the assurance levels are to be met by implementing the LoA's, the recognition and notification are mere formal procedures, that adhere to the reputation aspect of Member States. Also the obligation to inform other Member States when there is a security breach is the notified eID solution (eIDAS, Article 10) and the liability for the notifying Member State in case of "damage caused intentionally or negligently to any natural or legal person" (eIDAS, Article 11) are characteristics of reputation. Overall it shows that the goal of the eIDAS Regulation is to seek trust in eID solutions by the reputation aspect.

## 4.8 Quantitative results

After performing the whole policy analysis, it is interesting to look at the quantitative results of the analysed elements. This quantitative analysis shows how many times trust elements are found and hence how many times trust can be ensured throughout the analysed regulations. In Table 5 the results are shown.

*Table 5 Quantitative analysis of the results*

| Policy | Total analysed elements | Number of analysed applicable elements for enrolment | | | | | Number of analysed applicable elements for authentication | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Compliance | Usability | Security | Privacy | Reputation | Compliance | Usability | Security | Privacy | Reputation |
| **ID-card** | 11 | 7 | 4 | 4 | 6 | 7 | 3 | 3 | 3 | 3 | 3 |
| **ICAO** | 7 | 6 | 6 | 5 | 4 | 7 | 5 | 6 | 5 | 4 | 7 |
| **eIDAS** | 8 | 8 | 5 | 5 | 5 | 8 | 8 | 5 | 5 | 5 | 8 |
| **LoA's** | 8 | 5 | 4 | 4 | | | 2 | 2 | 2 | | |
| **GDPR** | 3 | 3 | | | 3 | | 3 | | | 3 | |

From these numbers it can be seen that that the ID-card, ICAO and eIDAS regulations have a broad coverage of trust aspects, so these regulations can be used to ensure trust in all researched trust aspects of usability, security, privacy and reputation. The LoA's show that their elements can only be

used for ensuring usability and security and not for privacy or reputation. As the LoA's are like a technical implementation guidance to the eIDAS regulation, the focus on usability and security might be logical. Finally the GDPR has solely focus on the trust aspect of privacy, which is a direct result from its working area on the protection of personal data. In general these numerical results show that the analysed policies can be used to ensure trust by the different trust factors.

## 5. General discussion

From the whole policy analysis it shows that international standards form an important input to EU regulations. The ID-card itself is standardized by the ICAO, making it an electronic Machine Readable Travel Document. The usage of the biometric data on the ID-card as an eID solution, however seems not very standardized and also the eIDAS and its LoA's do not mention standards to obey to. For an eID solution that makes use of mobile biometrics, as proposed in this research, it might be good to look into international standards that are applicable to the subject matter. ENISA [2020] also mentions this and several researches look into the application of standards on biometric data protection, like Yang et.al. [2013], Buchmann et.al. [2013] and more recently Raja et.al. [2019]. It could benefit trust in biometric solutions, if these international standards would form part of policies.

The implementation of these standards and other protective measures is focussed on the authentication process, trying to make it more secure by preventing that an attacker can make use of the biometric data or the eID solution as a whole. But maybe the attacker is more interested in the value of the transaction that takes place *after* authentication, the transaction with eGovernment. The attacker could wait for the citizen to perform the authentication and just then launch the attack, for example on the mobile device that is being used by the citizen. It would make the whole effort of protecting the authentication process and the biometric data in it quite useless, and it would diminish trust in the transaction with eGovernment as a whole.

Still, the goal of this research is to investigate the implementation of a compliant eID solution, and from the policy analysis it is clear that some technical measures must be met. The most important one is to make proper use of the cryptographic techniques of the ID-card and the biometric data on it. Another technical measure that follows from the policy analysis, is the need for a centrally accessible activation register of the eID solution, which also serves for suspension and revocation status. Having this centralised register makes way to possibly new attacks on the eID solution as a whole, like for example Denial-of-Service attacks. So, the question remains if the proposed solution in this research could be resistant to an attacker with "high attack potential", as defined in the eIDAS and its LoA's.

Not only technical implementation measures must be met, also other measures can be taken to ensure trust in the proposed solution. Awareness is mentioned as a possible instrument, as it gives insight to the citizen of the outcome and risk of the proposed solution. Reputation shows not to be only a technological trust aspect, but also a regulatory instrument, as the eIDAS Regulation seeks to enhance trust in eID solutions by using reputation. In general it shows that the policies seek more to enhance trust in organisations delivering the technology than in technology itself, a difference in trust that has been investigated by Lankton & McKnight [2011]. Also in a later work it shows that choosing the right trust attributes is important for trust to be effective (Lankton et.al. [2015]), so policies could be made more effective by putting more emphasis on technology trust. Maybe the technology neutral approach of the eIDAS Regulation has been counterproductive to its effect on trust.

A rather difficult aspect to implement seems to be dignity of the person, which is addressed explicitly for the ID-card during the enrolment process. Although for the eID solution that makes use of the ID-card during the authentication process, dignity is not found as an explicit aspect, it forms part of the always evolving privacy discourse (Bloustein [1964]). The GDPR, being the main privacy regulation in the EU, therefore should uphold the dignity of the person in other regulations as well. For the eIDAS this is accomplished by referencing the GDPR, and implementing the GDPR should provide for sufficient privacy. For eID solutions, research has been done if additional privacy measures are still

necessary, for example against profiling, and shows that these decisions may vary per Member State (Tsakalakis [2020]).

The most important decision to make on privacy for a Member State, however, is whether the facial image on the ID-card can be used by the citizen themself, for an eID solution in the authentication process for eGovernment. There are two aspects to this decision, that are addressed separately. The first is that of usage by the citizen themself. From the analysis in section 4.4 it shows that a Member State could choose to protect the facial image with additional cryptographic techniques, leaving it inaccessible to the holder of the card. Only authorised staff with authorised equipment could then access the data. Current implementations of the ID-card show however that most Member States choose to have the facial image readily available to the holder of the ID-card (Szádeczky [2018]). It could be discussed whether this is a proper protection of biometric data, especially comparing it to the protection of fingerprints on the same ID-card, which is at a higher level of access control (ENISA [2020]).

The other aspect is whether the facial image, once read from the ID-card, can be used for an eID solution in the authentication process for eGovernment. This is about the purpose of the usage and adheres to the analysis in section 4.6. If the purpose is required by law, it could be a granted exception to the prohibition of processing biometric data in the GDPR. Another possible exception lies within the explicit consent of the citizen to use the biometric data, but then the discussion is how this consent should be implemented and to what extent. In an extensive analysis, Kindt [2018] shows that deciding on the use of biometric data already starts with the collection of that data, which in the proposed solution in this research is at the enrolment process of the ID-card.

Both aspects show that EU Member States should choose how to protect the storage as well as the usage of the biometric data on the ID-card, and decide on it before issuing national ID-cards. It would be interesting to see how all Member States have gone through this process of national decision making but is left for further research. For the scope of this research it is good to know that implementation of the proposed solution is dependent on possibly different implementations of the ID-card.

Also the eIDAS Regulation is implemented on a Member State level, using the constructs of mutual recognition and notification, as analysed in section 4.7. Combined with the interoperability of the resulting eID solutions in the transnational EU context of eGovernment, it makes the proposed solution in this research only viable if it is implemented under the auspices of a Member State. This political positioning makes that implementing an eID solution is more than just technical implementation and compliance (van Dijck & Jacobs [2020]), which is also shown in this research. Further research could show how Member States are dealing with eID solutions with mobile biometrics. ENISA [2020] already gives some insights.

In the meantime the EU has evaluated the eIDAS Regulation[6] and has come with a revision proposal[7]. From the explanatory memorandum it is understood that the evaluation has led to the insight that the market needs have changed to a more attribute-based, wallet-type digital identity, which is also the type of solution that is proposed by van Dijck & Jacobs [2020]. This shift in identity management is taking place while the “old type” of identity management, with multi-factor authentication and biometrics being the most difficult to implement factor, is not fully implemented yet. Also the question of how such a new type of digital identity should be protected from being used by another

[6] https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-evaluation-regulation (accessed 27-1-2023)

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281 (accessed 27-1-2023)

person is not easily answered. This research shows that, despite the difficulties, implementing an eID solution with mobile biometrics might be the answer to the difficult problem of verifying someone's identity over the Internet. And there still might be time, as the oldest authentication factor, a password, is still being used extensively.

## 6. Conclusion

The main construct in this research has been trust, which has been defined as a positive effect on the expected outcome and the acceptance of risk of a transaction in a certain context. For the context of transactions with government it showed that identity verification is an important step in those transactions, both in the physical as in the digital world. In the digital world the identity verification is done with multi-factor authentication, of which biometrics is the technology factor that resembles the face-to-face identity verification of the physical world. For people to trust this technology, and willing to use it, the trust factors of usability, security, privacy and reputation are found to be the main constructs to implement.

Within the EU, transnational identity verification in the physical world is possible with the ID-card. By matching a live facial image of the user with the photo stored on the chip of the ID-card it should be possible to have a trustful identity verification in the digital world. The design of such an eID solution with mobile biometrics has been presented, but the question arose whether this solution would be compliant to EU legislation and if it would implement the mentioned trust factors. This research question has been investigated by conducting a policy analysis on the applicable EU legislation and look for compliance as well as ways for implementing the trust factors.

The policy analysis revealed that technical implementation aspects are highly compliant and also ensure various trust aspects of technology, mainly usability, security and privacy. The trust aspect of reputation is found to be more likely an aspect of the organisation implementing the whole solution and for eID solutions in particular, the eIDAS Regulation is built upon the construct of reputation. Also non-technical implementation aspects are found to be important to enhance trust, like awareness and dignity. In general all trust aspects have been found in the analysed policies, but their focus seems on trust in organisations and not in (biometric) technology. Therefore future revisions of the policies could still have more emphasis on technology trust, so that citizens can really perceive a positive effect on trust in biometric technology.

Also new questions have risen during the research. The most difficult ones to answer are about the privacy of the biometric data on the ID-card: is the storage and usage of the biometric data compliant to the GDPR and in which way could explicit user consent bypass the objections of processing these data. These are left for further research.

Although the scope of the research was the EU and transnational identity verification, a complicating issue that was found in this research is that all implementation is done at the Member State level, both for the ID-card as for the eID solution. Combined with the GDPR implementation and further restrictions on personal data at the Member State level, this makes that the research should be iterated for each Member State.

Nevertheless, the findings of this research can be used to enhance the discussion about the implementation of biometric identity verification in the digital world. The constructs of usability, security, privacy and reputation can be used as guidance to deliver a trustworthy eID solution with mobile biometrics and with it ensure trust in transactions with eGovernment.

**References**

Abrial, A., Bouvier, J., Renaudin, M., Senn, P., & Vivet, P. (2001). A new contactless smart card IC using an on-chip antenna and an asynchronous microcontroller. IEEE Journal of Solid-State Circuits, 36(7), 1101-1107.

Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S., & Reich, C. (2015, September). Security, privacy and usability–a survey of users' perceptions and attitudes. In International conference on trust and privacy in digital business (pp. 153-168). Springer, Cham.

Alshamari, M. (2016). A review of gaps between usability and security/privacy. International Journal of Communications, Network and System Sciences, 9(10), 413-429.

Andraško, J. (2017). MUTUAL RECOGNITION OF ELECTRONIC IDENTIFICATION MEANS UNDER THE EIDAS REGULATION AND ITS APPLICATION ISSUES. AD ALTA: journal of interdisciplinary research, 7(2).

Andraško, J. (2018). Identification and authentication of persons in cyberspace in selected states. International and Comparative Law Review, 18(1), 199-216.

Arner, D. W., Zetzsche, D. A., Buckley, R. P., & Barberis, J. N. (2019). The identity challenge in finance: from analogue identity to digitized identification to digital KYC utilities. European business organization law review, 20(1), 55-80.

Berg, van den, B. & Keymolen, E. (2017) Regulating security on the Internet: control versus trust, International Review of Law, Computers & Technology, 31:2, 188-205, DOI: 10.1080/13600869.2017.1298504

Bloustein, E. J. (1964). Privacy as an aspect of human dignity: An answer to Dean Prosser. NYUL rev., 39, 962.

Buchmann, N., Peeters, R., Baier, H., & Pashalidis, A. (2013, September). Security considerations on extending PACE to a biometric-based connection establishment. In 2013 International Conference of the BIOSIG Special Interest Group (BIOSIG) (pp. 1-13). IEEE.

Busch, C., Nouak, A., Zhou, X., van der Veen, M., Deravi, F., & Suchier, J. M. (2007). Towards unattended and privacy protected border control. In 2007 Biometrics symposium (pp. 1-6). IEEE.

Caplan, J., Torpey, J., & Torpey, J. C. (Eds.). (2001). Documenting individual identity: The development of state practices in the modern world. Princeton University Press.

Camp, J. L. (2004). Digital identity. IEEE Technology and society Magazine, 23(3), 34-41.

Casadesus-Masanell, R. (2004). Trust in agency. Journal of Economics & Management Strategy, 13(3), 375-404.

Casaló, L. V., Flavián, C., & Guinalíu, M. (2007). The role of security, privacy, usability and reputation in the development of online banking. Online Information Review.

Collings, T. (2008). Some thoughts on the underlying logic and process underpinning Electronic Identity (e-ID). Information security technical report, 13(2), 61-70.

Das, T. K., & Teng, B. S. (2001). Trust, control, and risk in strategic alliances: An integrated framework. Organization studies, 22(2), 251-283.

Datta, A. K., Lee, H. C., Ramotowski, R., & Gaensslen, R. E. (2001). Advances in fingerprint technology. Chapter 1 "History and development of fingerprinting". CRC press.

Dijck, van, J., & Jacobs, B. (2020). Electronic identity services as sociotechnical and political-economic constructs. new media & society, 22(5), 896-914.

ENISA (March 2020). eIDAS compliant eID solutions - Security Considerations and the Role of ENISA. https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions (accessed 27-1-2023).

EU 910/2014. Regulation (EU) of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. https://eur-lex.europa.eu/eli/reg/2014/910/oj (accessed 27-1-2023).

EU 2015/1502. Commission Implementing Regulation (EU) of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. https://eur-lex.europa.eu/eli/reg_impl/2015/1502/oj (accessed 27-1-2023).

EU 2016/679. Regulation (EU) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed 27-1-2023).

EU 2019/1156. Regulation (EU) of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement. https://eur-lex.europa.eu/eli/reg/2019/1157/oj (accessed 27-1-2023).

Feldman, R. (2002). Considerations on the emerging implementation of biometric technology. Hastings Comm. & Ent. LJ, 25, 653.

Figarella, M. (2017). Global consensus emerges on biometric data protection. Biometric Technology Today, 2017(10), 5-7.

Flavián, C., Guinalíu, M., & Gurrea, R. (2006). The role played by perceived usability, satisfaction and consumer trust on website loyalty. Information & management, 43(1), 1-14.

Geteloma, V., Ayo, C. K., & Goddy-Wurlu, R. N. (2019). A proposed unified digital id framework for access to electronic government services. In Journal of Physics: Conference Series (Vol. 1378, No. 4, p. 042039). IOP Publishing.

Gofman, M., Mitra, S., Bai, Y., Choi, Y. (2019). Security, Privacy, and Usability Challenges in Selfie Biometrics. In: Rattani, A., Derakhshani, R., Ross, A. (eds) Selfie Biometrics. Advances in Computer Vision and Pattern Recognition. Springer, Cham.

Hall, R. (1993). The world of William Notman: the nineteenth century through a master lens. David R. Godine Publisher.

Hoffman, L. J., Lawson-Jenkins, K., & Blum, J. (2006). Trust beyond security: an expanded trust model. Communications of the ACM, 49(7), 94-101.

ICAO Document 9303, Machine Readable Travel Documents, Part 9 — Deployment of Biometric Identification and Electronic Storage of Data in MRTDs, Eight Edition (2021). ISBN 978-92-9265-381-1.

Published on ICAO website https://www.icao.int/publications/documents/9303_p9_cons_en.pdf (accessed 27-1-2023).

ICAO Technical Report Portrait Quality (Reference Facial Images for MRTD) (2018, April). Version 1.0. Published on ICAO website https://www.icao.int/Security/FAL/TRIP/Documents/TR%20-%20Portrait%20Quality%20v1.0.pdf (accessed 27-1-2023).

Isobe, Y., Seto, Y., & Kataoka, M. (2001, January). Development of personal authentication system using fingerprint with digital signature technologies. In Proceedings of the 34th Annual Hawaii International Conference on System Sciences (pp. 9-pp). IEEE.

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. Communications of the ACM, 43(2), 90-98.

Jain, A. K., & Nandakumar, K. (2012). Biometric authentication: System security and user privacy. Computer, 45(11), 87-92.

Johansen, J., Fischer-Hübner, S. (2019): Making GDPR Usable: A Model to Support Usability Evaluations of Privacy. In: Friedewald, M., Önen, M., Lievens, E., Krenn, S., Fricker, S. (eds.) Privacy and Identity Management. Data for Better Living: AI and Privacy, IFIP Advances in Information and Communication Technology, vol. 576, pp. 275–291. Springer International Publishing.

Kanak, A., & Sogukpinar, I. (2017). BioTAM: a technology acceptance model for biometric authentication systems. IET Biometrics, 6(6), 457-467.

Kindt, E. J. (2018). Having yes, using no? About the new legal regime for biometric data. Computer law & security review, 34(3), 523-538.

Kitsing, M. (2018, April). The Janus-faced approach to governance: a mismatch between public sector reforms and digital government in Estonia. In Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance (pp. 59-68).

Kleist, V. F. (2007). Building technologically based online trust: Can the biometrics industry deliver the online trust silver bullet?. Information Systems Management, 24(4), 319-329.

Kramer, I. R. (1989). The Birth of Privacy Law: A Century Since Warren and Brandeis. Cath. UL Rev., 39, 703.

Krivachy, T. (1985, April). The chipcard—an identification card with cryptographic protection. In Workshop on the Theory and Application of Cryptographic Techniques (pp. 200-207). Springer, Berlin, Heidelberg.

Kubicek, H., & Noack, T. (2010). Different countries-different paths extended comparison of the introduction of eIDs in eight European countries. Identity in the Information Society, 3(1), 235-245.

Lah, U., Lewis, J. R., & Šumak, B. (2020). Perceived usability and the modified technology acceptance model. International Journal of Human–Computer Interaction, 36(13), 1216-1230.

Lankton, N. K., & McKnight, D. H. (2011). What does it mean to trust facebook? Examining technology and interpersonal trust beliefs. ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 42(2), 32-54.

Lankton, N. K., McKnight, D. H., & Tripp, J. (2015). Technology, humanness, and trust: Rethinking trust in technology. Journal of the Association for Information Systems, 16(10), 1.

Lee, Y., Kozar, K. A., & Larsen, K. R. (2003). The technology acceptance model: Past, present, and future. Communications of the Association for information systems, 12(1), 50.

Maguire, M. (2009). The birth of biometric security. Anthropology today, 25(2), 9-14.

Miltgen, C. L., Popovič, A., & Oliveira, T. (2013). Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context. Decision support systems, 56, 103-114.

National Research Council. (2010). Toward Better Usability, Security, and Privacy of Information Technology: Report of a Workshop. National Academies Press.

Oliver, P., & Roth, W. H. (2004). Internal Market and the Four Freedoms, The. Common Market L. Rev., 41, 407.

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. Cryptography, 2(1), 1.

Oostveen, A. M., & Lehtonen, P. (2018). The requirement of accessibility: European automated border control systems for persons with disabilities. Technology in Society, 52, 60-69.

Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. IEEE security & privacy, 1(2), 33-42.

Preuveneers, D., Joos, S., & Joosen, W. (2021, September). AuthGuide: Analyzing Security, Privacy and Usability Trade-Offs in Multi-factor Authentication. In International Conference on Trust and Privacy in Digital Business (pp. 155-170). Springer, Cham.

Raja, K. B., Raghavendra, R., Stokkenes, M., & Busch, C. (2019). Biometric template protection on smartphones using the manifold-structure preserving feature representation. In: Rattani, A., Derakhshani, R., Ross, A. (eds) Selfie Biometrics. Advances in Computer Vision and Pattern Recognition. Springer, Cham..

Rattani, A., Derakhshani, R., Ross, A. (2019). Introduction to Selfie Biometrics. In: Rattani, A., Derakhshani, R., Ross, A. (eds) Selfie Biometrics. Advances in Computer Vision and Pattern Recognition. Springer, Cham.

Rao, Y. S., Sukonkina, Y., Bhagwati, C., & Singh, U. K. (2008, November). Fingerprint based authentication application using visual cryptography methods (improved id card). In TENCON 2008-2008 IEEE Region 10 Conference (pp. 1-5). IEEE.

Rissanen, T. (2010). Electronic identity in Finland: ID cards vs. bank IDs. Identity in the Information Society, 3(1), 175-194.

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. Journal of Information System Security, 10(3).

Schaar, P. (2010). Privacy by design. Identity in the Information Society, 3(2), 267-274.

Schwartz, P. M. (2019). Global data privacy: The EU way. NYUL Rev., 94, 771.

Schouten, B., & Salah, A. A. (2008, December). Empowering the end-user in biometrics. In 2008 10th International Conference on Control, Automation, Robotics and Vision (pp. 1357-1360). IEEE.

Scott, M., Acton, T., and Hughes, M. (2005). An Assessment of Biometric Identities as a Standard for E-Government Services. International Journal of Standards and Services., Vol 1 Issue 1

Shankar, A., Jebarajakirthy, C., & Ashaduzzaman, M. (2020). How do electronic word of mouth practices contribute to mobile banking adoption?. Journal of Retailing and Consumer Services, 52, 101920.

Solove, D. J. (2016). A brief history of information privacy law. Proskauer on privacy, PLI.

Szádeczky, T. (2018). Enhanced functionality brings new privacy and security issues–an analysis of eID. Masaryk University Journal of Law and Technology, 12(1), 3-27.

Tarafdar, M. (2005). Analyzing the influence of web site design parameters on web site usability. Information Resources Management Journal (IRMJ), 18(4), 62-80.

Thomas, P. A. (1995). Identity cards. The Modern Law Review, 58(5), 702-713.

Tsakalakis, N. (2020). Analysing the impact of the GDPR on eIDAS: Supporting effective data protection by design for cross-border electronic identification through unlinkability measures (Doctoral dissertation, University of Southampton).

Tsap, V., Pappel, I., & Draheim, D. (2019, August). Factors affecting e-ID public acceptance: a literature review. In International Conference on Electronic Government and the Information Systems Perspective (pp. 176-188). Springer, Cham.

Warren S, Brandeis L (1890). Harvard Law Review December 1890.

Wisman, T. (2015). Willems: Giving Member States the Prints and Data Protection the Finger. European Data Protection Law Review (Internet), 1(3), 245–248.

Yang, B., Busch, C., Bringer, J., Kindt, E., Belser, W. R., Seidel, U., ... & Aukrust, M. (2013, November). Towards standardizing trusted evidence of identity. In Proceedings of the 2013 ACM workshop on Digital identity management (pp. 63-72).

**Annex 1 – Analysis of applicable policies**

This annex contains all policies mentioned in the EU 2019/1156 regulation and analyses them to be put in or out of scope of the designed solution.

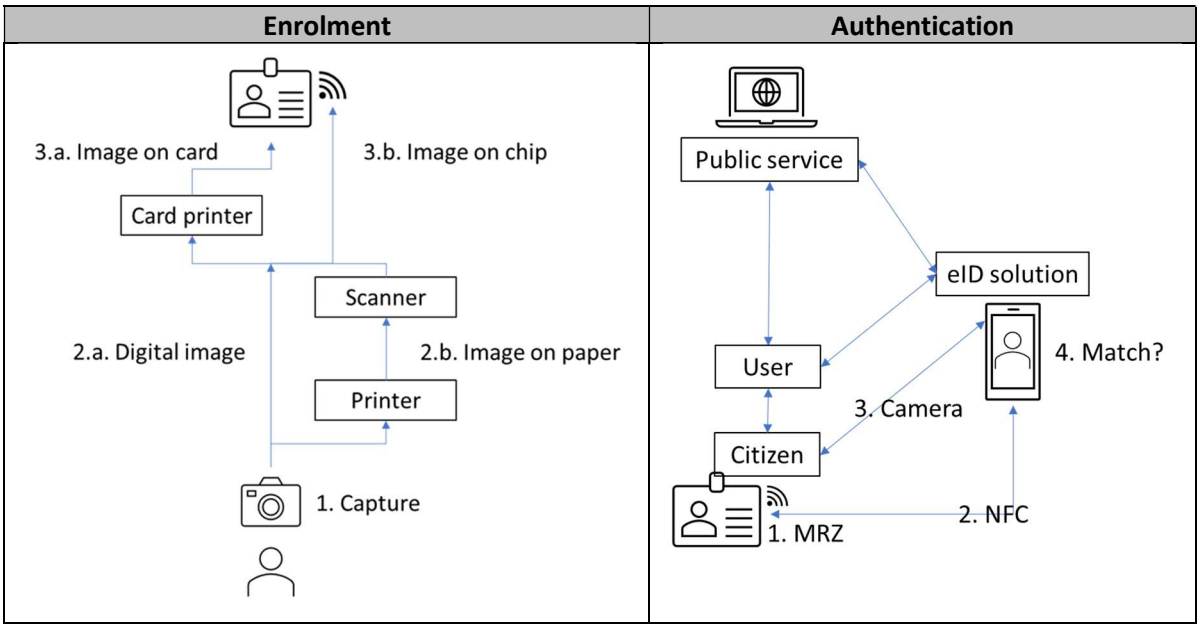
| Policy / regulation | Analysis | Verdict |
|---|---|---|
| EU 2019/1156. Regulation on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement | This is the main *regulation* in scope of this research | Analysed |
| ICAO Document 9303, Machine Readable Travel Documents, Part 9 — Deployment of Biometric Identification and Electronic Storage of Data in MRTDs | This is the main *standard* in scope of this research. Referenced ISO standards within this document are not analysed further. | Analysed |
| Preamble 1: Treaty on the European Union (TEU) and Treaty on the Functioning of the European Union (TFEU) | It is the foundation of all EU regulation. | Not analysed |
| Preamble 2-3-4: Directive 2004/38/EC of the European Parliament and of the Council gives effect to the right of free movement. Article 45 of the Charter of Fundamental Rights of the European Union (the Charter) also provides for freedom of movement and residence. | Freedom of movement entails the right to exit and enter Member States with a valid identity card or passport. This is the origin of the EU 2019/1157 regulation on ID-cards. | Not analysed |
| Preamble 6: EU Commission Communication of 14 September 2016 entitled 'Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders'. | Secure travel and identity documents are crucial whenever it is necessary to establish without doubt a person's identity, and announced that it would be presenting an action plan to tackle travel document fraud. So the result is the EU 2019/1157. | Not analysed |
| Preamble 7: Commission's Action Plan of 8 December 2016 to strengthen the European response to travel document fraud. | Less secure national identity cards issued by Member States are the most frequently detected false documents used for intra-Schengen travel. | Not analysed |
| Preamble 9-10: EU Citizenship Report (2017) | Committed itself to analysing policy options to improve the security of identity cards and residence documents. So the result is the EU 2019/1157. | Not analysed |
| Preamble 14: Travel documents compliant with part 5 of International Civil Aviation Organization (ICAO) Document 9303 on Machine Readable Travel Documents, (seventh edition, 2015) | These documents are not eMRTDs | Not analysed |
| Preamble 15: Regulation (EU) No 910/2014 of the European Parliament and of the Council which provides for Union-wide mutual recognition of electronic identifications in access to public services. | Improved security of identity cards should ensure easier identification and contribute to better access to services. | Analysed |

| | | |
|---|---|---|
| Preamble 25:<br>Council Regulation (EC) No 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals (OJ L 157, 15.6.2002, p. 1).<br>Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).<br>Council Regulation (EC) No 1683/95 of 29 May 1995 laying down a uniform format for visas (OJ L 164, 14.7.1995, p. 1). | Residence permits and visas are not in scope. | Not analysed |
| Preamble 26: the Charter, the Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe and the United Nations Convention on the Rights of the Child. | Member States should ensure that the best interest of the child is a primary consideration throughout the collection procedure. To that end, qualified staff should receive appropriate training on child-friendly practices for the collecting of biometric identifiers.<br>This preamble is within the scope of the research but the mentioned documents are too broad. | Not analysed |
| Preamble 34: Directive 2004/38/EC | Already addressed | Not analysed |
| Preamble 35: UN Charter and Convention on the Rights of Persons with Disabilities. | Member States are encouraged to work with the Commission to integrate additional features that render identity cards more accessible and user-friendly to people with disabilities, such as visually impaired persons.<br>Member States are to explore the use of solutions, such as mobile registration devices, for the issuance of identity cards to persons incapable of visiting the authorities responsible for issuing identity cards.<br>This preamble is within the scope of the research but the mentioned documents are too broad. | Not analysed |
| Preamble 37: Regulation (EU) 2017/1954 of the European Parliament and of the Council of 25 October 2017 amending Council Regulation (EC) No 1030/2002 laying down a uniform | Residence permits for third-country nationals are not in scope. | Not analysed |

| | | |
|---|---|---|
| format for residence permits for third-country nationals (OJ L 286, 1.11.2017, p. 9). | | |
| Preamble 38: Directive 2004/38/EC | Already addressed | Not analysed |
| Preamble 40-41-43: Regulation (EU) 2016/679 of the European Parliament and of the Council | Member States should be responsible for the proper processing of biometric data, from collection to integration of the data on the highly secure storage medium, in accordance with Regulation (EU) 2016/679, the GDPR. | Analysed |
| Article 3 – Paragraph 1: Regulation (EU) 2017/1954 of the European Parliament and of the Council of 25 October 2017 amending Council Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals. | Already addressed | Not analysed |
| Article 3 – Paragraph 5-6: Commission Implementing Decision C(2018) 7767 of 30 November 2018 laying down the technical specifications for the uniform format for residence permits for third country nationals and repealing Decision C(2002) 3069. | Residence permits for third-country nationals are not in scope. | Not analysed |
| Article 11 – Paragraph 1-2-3: Regulation (EU) 2016/679 | Already addressed | Analysed |

**Annex 2 – Policy analysis of the proposed solution**

This annex contains all analysed elements from the applicable policies within scope of the proposed solution. For easy reference the solution of Figures 3 (process of enrolment) and 4 (process of authentication) are repeated, as well as the policies of Table 1.




| Reference | Date | Common name | Working area |
|---|---|---|---|
| EU 2019/1157 | 20 June 2019 | ID-card | Strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement |
| ICAO Document 9303 Part 9 | 2021 | ICAO | Deployment of Biometric Identification and Electronic Storage of Data in MRTDs |
| EU 910/2014 | 23 July 2014 | eIDAS | Electronic identification and trust services for electronic transactions in the internal market |
| EU 2015/1502 | 8 September 2015 | LoA's | Minimum technical specifications and procedures for assurance levels for electronic identification |
| EU 2016/679 | 27 April 2016 | GDPR | Protection of natural persons with regard to the processing of personal data and on the free movement of such data |

| 1 | **Policy:** ID-card | **Reference:** Article 3 Security standards/format/specifications – Paragraph 1 |
|---|---|---|

1. Identity cards issued by Member States shall be produced in ID-1 format and shall contain a machine-readable zone (MRZ). Such identity cards shall be based on the specifications and minimum security standards set out in ICAO Document 9303 and shall comply with the requirements set out in points (c), (d), (f) and (g) of the Annex to Regulation (EC) No 1030/2002 as amended by Regulation (EU) 2017/1954.

Preamble (23): The specifications of ICAO Document 9303 which ensure global interoperability including in relation to machine readability and use of visual inspection should be taken into account for the purpose of this Regulation.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | Not applicable | This element is analysed because the MRZ (or the data in it) is needed in the authentication process to get access to the storage medium (electronic chip), so it forms part of the technology used in the solution.<br><br>The ICAO Document 9303 is referenced as a (security) standard. However, the stipulation says “shall be based on”, which is different than “compliant to”. Probably this is because the ICAO Document 9303 is not approved law/legislation. Preamble (23) does not provide more information, as it states “should be taken into account”.<br><br>Supposedly all identity cards issued are compliant to this policy, so for this research the whole ICAO Document 9303 is not relevant anymore, and only Part 9 “Deployment of Biometric Identification and Electronic Storage of Data in MRTDs” is used. The Part 9 document published at ICAO is already eighth edition (2021) and that is a general problem of standards, they evolve independently of regulations. The discussion could be whether a new version of ICAO Document 9303 is automatically incorporated in the regulation.<br><br>For the authentication process, the MRZ is supposed to be compliant, and “based on” the ICAO standard. |
| **Trust factor Usability:** | Not applicable | The ID-1 format and the MRZ are aspects to be analysed for usability.<br><br>The ID-1 format is not specified nor referenced within this policy (!?), so an Internet search was performed to reveal that the ID-1 format is specified in the international *standard* ISO/IEC-7810, indicating the physical dimensions of the card. The ID-1 format is also used for banking cards and therefore also known as “credit card size”. The usability of this card size is well-known to most citizens as most people use banking cards in their daily lives. Using this format for the identity card therefore has a positive effect on usability. However, being a smaller format than a passport for example, some people might have (negative) usability issues because of easy misplacement or loss of the card, which causes a lot of additional problems in security and privacy. (relationship!)<br><br>The MRZ has in its name already a “negative” aspect of usability, because it says that it is “machine readable”, so it is likely that a citizen would think that it is not human readable. However, the MRZ is just a few lines of text printed in an special Optical Character Recognition (OCR) font. With OCR technology (used with a photo camera or other scanning device) it is possible to have the device “read” (recognize) the characters and process them further. In the MRZ some main data elements of the identity card are present (as specified in ICAO Document 9303), among which the document number, the birth date and the expiry date. These three data elements are exactly the only ones needed to get access to the storage medium (electronic chip access by BAC or PACE as specified |

| | | |
|---|---|---|
| | | in ICAO Document 9303), something that is not known to most people using electronic Machine Readable Travel Documents (eMRTDs). So instead of scanning the MRZ with a camera, it is also possible to use the three data elements by typing them in manually, which could have a positive usability effect on citizens. In ICAO document 9303 there is mentioned another method of access to the storage medium, by the Card Access Number, which is a 6-digit number: "In contrast to the MRZ (Document Number, Date of Birth, Data of Expiry) the CAN has the advantage that it can easily be typed in manually." So in the ICAO document there is thought about usability.<br><br>Another positive aspect of the usability of the MRZ lies within the used font, which is mostly bigger and easier to read for a human than the normal data elements on the identity card. So actually the MRZ should be named differently, maybe "Easy Readable Data (ERD)", to indicate its usability. |
| **Trust factor Security:** | Not applicable | Security is an important aspect of the MRZ, because its data is needed to get access to the storage medium. However, this aspect of security is not mentioned in this stipulation. A citizen could think that the MRZ is not very important for the security of the identity card and be careless about its use. This has a negative effect on the whole security of the card. Attacks on the identity card could be possible, for example by "shoulder-surfing" the MRZ with a camera or just by convincing the citizen that it is no problem to scan the MRZ. Subsequently, the attacker could get access to the storage medium as well. Security awareness might be needed to have a positive effect.<br><br>The security aspect is even more negative when it is known that only 3 data elements of the MRZ are actually needed or even the CAN code (see Compliance). The ID-1 format of the card is prone to easy misplacement or loss and can give an attacker opportunity to get access to the card and read the personal data. |
| **Trust factor Privacy:** | Not applicable | Privacy of the MRZ is similar to the security of it. Many people might not be aware that the MRZ contains exactly the data as shown on the "normal" part of the identity card. So when people make a photocopy of their identity card (for use in identity verification, but out of scope in this research), they might remember that it is good practice to blacken certain data on the photocopy[8] but forget to blacken the MRZ. The photocopy could then still be used to retrieve personal data that was supposed to be private. Awareness of this issue could have a positive effect.<br><br>The privacy aspect is even more negative when it is known that only 3 data elements of the MRZ are actually needed or even the CAN code (see Compliance). The ID-1 format of the card is prone to easy misplacement or loss and can give an attacker opportunity to get access to the card and read the personal data. |
| **Trust factor Reputation:** | Not applicable | MRZ as technology in eMRTDs seems not be known widely, nor the standards on it that are held by ICAO. Even the ICAO as organisation is not very known, although almost every citizen in the world has to do with its standards when travelling by air. Therefore it is not likely that reputation has an negative effect on the MRZ itself. However, using the MRZ, by scanning the whole area of by manually typing in the data, can be difficult for some citizens, and this might lead to reputation problems. Tips and tricks about the usage of the MRZ could have a positive effect. |

[8] https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/vraag-en-antwoord/fraude-voorkomen-met-kopie-id-bewijs

| **2** | **Policy:** ID-card | **Reference:** Article 3 Security standards/format/specifications – Paragraph 5-6 |
|---|---|---|

5. Identity cards shall include a highly secure storage medium which shall contain a facial image of the holder of the card and two fingerprints in interoperable digital formats. For the capture of biometric identifiers, Member States shall apply the technical specifications as established by Commission Implementing Decision C(2018) 7767.
6. The storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data. The data stored shall be accessible in contactless form and secured as provided for in Implementing Decision C(2018) 7767. Member States shall exchange the information necessary to authenticate the storage medium and to access and verify the biometric data referred to in paragraph 5.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | This element is analysed because the storage medium is used to *store* the biometric data, which are captured in the enrolment process, forming part of the technology used in the solution.<br><br>The following reference is out of scope (residence permits):<br>- Commission Implementing Decision C(2018) 7767 of 30 November 2018 laying down the technical specifications for the uniform format for residence permits for third country nationals and repealing Decision C(2002) 3069.<br>This might leaves the whole part about the capture of biometric identifiers out of scope.<br>When looking at preamble 18:<br>The storage of a facial image and two fingerprints ('biometric data') on identity and residence cards, as already provided for in respect of biometric passports and residence permits for third-country nationals, represents an appropriate combination of reliable identification and authentication with a reduced risk of fraud, for the purpose of strengthening the security of identity and residence cards.<br>makes it seem that they apply it to identity cards as well! So it is in scope!? It seems that the EU wanted to reuse this regulation?<br><br>Annex III<br>Biometrics Deployment of EU-residence permits for third country nationals<br>refers to ICAO (and ISO) standards.<br>The process of capturing (enrolment) should then comply to these standards. This process is in standards, not in regulation! The discussion would be how does the regulation verify these | This element is analysed because the storage medium is used to *read* the biometric data during the authentication process, forming part of the technology used in the solution.<br><br>For the solution to be able to read the biometric data, specifically the digital format is important. A question could be raised whether the part "in interoperable digital formats" applies to both the facial image and the two fingerprints, or that it applies only to the two fingerprints.<br><br>a facial image of the holder of the card and two fingerprints – in interoperable digital formats<br>or<br>a facial image of the holder of the card – and two fingerprints in interoperable digital formats<br><br>In Annex III of the implementing Decision it is stipulated in detail what the "interoperable digital formats" are:<br>"The face is to be stored as a compressed IMAGE FILE, not as vendor specific template." And for the compliance is referred to ICAO Document 9303. The question here would be why the ICAO Document is not referenced!?<br>Part 9: "Requirements to capture and encoding of face images are specified in ISO/IEC 39794-5, Annex D.1."<br>So other standards are referenced.<br><br>Eventually several standards are used for the whole eMRTD solution proposed by ICAO. The discussion would be how does the regulation verify these standards? Or is it just about trust in the organisations? (So the EU trusts the ICAO, the ICAO trusts the ISO, etc.) |

| | | |
|---|---|---|
| | standards? Or is it just about trust in the organisations? (So the EU trusts the ICAO, the ICAO trusts the ISO, etc.) | |
| **Trust factor Usability:** | The capture of biometric identifiers …<br><br>Process in Figure 3. Can everybody do this? For example very small babies that need to travel?! They cannot comply to the standards.<br><br>Within this whole process can also be loss of quality of the captured image. Is the final photo on the chip still of enough quality to do the authentication process?<br><br>Verification at enrolment whether the photo really matches (digitally) with the person, so that the photo will work afterwards. But can it be done at that same moment? Is the final photo that goes on the chip available at enrolment? | The data stored shall be accessible in contactless form …<br><br>Process in Figure 4. But how can it be used? The NFC capabilities of the "contactless form" are not mentioned in the whole policy. Again it is in the standards!<br><br>Not everybody has a smartphone with NFC capabilities, so these citizens cannot use the solution.<br><br>Discussion could be:<br>Processes (with technology) are being "standardized". So usability aspects are in the standards. But standards might "forget" about special groups, at least standards are not applicable to everybody (not everybody is standard).<br><br>Is the final photo on the chip of enough quality to do the authentication process? |
| **Trust factor Security:** | The security aspect of the enrolment process (capture) is not mentioned. The discussion could be about how the data from the enrolment process goes to the chip manufacturer and into the chip. All these things are in the standards, not in this policy. | *highly secure* storage medium<br>The storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data. The data stored shall be accessible in contactless form and secured …<br><br>The term "highly secure" is very vague and not defined. Also the reason why it must highly secure is not mentioned in paragraph 5. In paragraph 6 however, the reason is stated: "to guarantee the integrity, the authenticity and the confidentiality of the data". It could be discussed why only these CIA aspects of security and not just mention "security".<br><br>The stipulation "shall be accessible" does not mention to whom and for what purpose. (This is mentioned in article 11 – par.3). But that it has to be accessible means that there might be many security issues. The term "and secured" is not very specific on how and when. Supposedly it is after the data is accessed in contactless form, so during and after the NFC reading process. However this is not described in detail here, and again might be in the standard. |

| | | |
|---|---|---|
| **Trust factor Privacy:** | The privacy aspect of the enrolment process (capture) is not mentioned. The discussion could be of how privacy is important in the enrolment process, e.g. no other people in the room, good equipment installation etc. | The privacy aspect of the authentication process is indirectly within the same terms as for security.<br>The term "highly secure" and "secured" could be because of privacy as well. The term "confidentiality of the data" is also because of privacy.<br>The discussion would be that it might be better to explicitly address the privacy aspect as reason of this stipulation.<br><br>A privacy aspect that is not in this element, but might be in others, is how the surroundings of the person doing the authentication are subject to privacy issues as well, e.g. can a person do the authentication while walking outside on the street where everybody can see them? Or only from home, on the couch so to say. |
| **Trust factor Reputation:** | Similar to MRZ, but same for both processes:<br>Chip technology in eMRTDs seems not to be known widely, nor the standards on it that are held by ICAO. Even the ICAO as organisation is not very known, although almost every citizen in the world has to do with its standards when travelling by air. Therefore it is not likely that reputation has an negative effect on the chip itself. However, chips might be associated with other data processing, for example banking or even "chipping" persons (like they do with pets) which has a surveillance purpose. So chips might have a bad reputation when it comes to mass surveillance. | |

| 3 | **Policy:** ID-card | **Reference:** Article 3 Security standards/format/specifications – Paragraph 7 |
|---|---|---|

7. Children under the age of 12 years may be exempt from the requirement to give fingerprints. Children under the age of 6 years shall be exempt from the requirement to give fingerprints. Persons in respect of whom fingerprinting is physically impossible shall be exempt from the requirement to give fingerprints.

Preambles
(27) Where difficulties are encountered in the collection of biometric identifiers, Member States should ensure that appropriate procedures are in place to respect the dignity of the person concerned. Therefore, specific considerations relating to gender, and to the specific needs of children and of vulnerable persons should be taken into account.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | This element is analysed because supposedly it is within the scope of "biometric data on the ID-card" (being facial image and fingerprints). However this stipulation is only for the fingerprints.<br><br>The point to make is that this stipulation has been chosen to be only applicable to fingerprints. Has thought been given to situations in which the facial image is also reason for exception? The preamble related to this stipulation (27) has this broader scope. For example the mentioned very small babies that need to travel in element 2?! They cannot comply to the standards, so you have to take away their freedom to travel (with their parents, in earlier days a child could be "annotated" in a parents' passport).<br><br>Compliance for the facial image is *not an issue* off course. | If there would be an exception for the facial image, it would be determined at the enrolment process. But then the ID-card could not be used for the authentication process.<br><br>Therefore not applicable |
| **Trust factor Usability:** | This element is about usability at the process of enrolment, trying to give a positive effect on special groups, younger children and other physically disabled persons. One thing is not mentioned here, that may be in the standards, is if person "temporarily" cannot capture biometric data. For example people who have a bruise in the face, or someone who is not in the exceptions in the standards, e.g. because of religious reasons (if the religion prohibits taking pictures, you cannot get an ID-card? here security / border protection will "win" from freedom of movement and freedom of religion) | Not applicable |
| **Trust factor Security:** | Not applicable, because there is no security aspect in this exemption. | Not applicable |
| **Trust factor Privacy:** | The reason for this stipulation is probably because of the privacy of the special groups. However this is not made explicit. The discussion could be that the policy can be made better if these aspects are made explicit. Explain in the policy why it is important, which is done in the preambles (27) But then the discussion is about whether the preambles form part of the policy or not. And if it is because of other regulations (GDPR?) it could be made explicit as well. | Not applicable |
| **Trust factor Reputation:** | The reputation of the process of taking fingerprints is in this element. It is "supposed" that smaller children should not, would not or can not take fingerprints. But this is not made explicit. The discussion could be that the policy can be made better if these aspects are made explicit. Explain in the policy why it is important, the preamble talks about the *dignity of the person*, which could be seen as a reputation aspect. | Not applicable |

| **4** | **Policy:** ID-card | **Reference:** Article 3 Security standards/format/specifications – Paragraph 10 |
|---|---|---|

10. Where Member States store data for electronic services such as e-government and e-business in the identity cards, such national data shall be physically or logically separated from the biometric data referred to in paragraph 5.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | The solution *re-uses* the (biometric) data from paragraph 5, for the purpose of e-government. This stipulation does not seem to prohibit it explicitly but it could be interpreted that if the data is used for other purposes it "shall be physically or logically separated". It also seems to be connected to Article 11 – Paragraph 6, which is about the purpose.<br><br>Also there is no reference to the compliance of electronic services, but this is referred to in preamble 15:<br>(15) This Regulation does not affect the use of identity cards and residence documents with eID function by Member States for other purposes, nor does it affect the rules laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council (4), which provides for Union-wide mutual recognition of electronic identifications in access to public services and which helps citizens who are moving to another Member State, by requiring mutual recognition of electronic identification means subject to certain conditions. Improved identity cards should ensure easier identification and contribute to better access to services.<br><br>Compliance is deferred to the Regulation EU 910/2014 (eIDAS). Therefore not applicable. | Same as enrolment |
| **Trust factor Usability:** | Since the compliance seems not applicable, this element is not analysed further. | Same as enrolment |
| **Trust factor Security:** | Since the compliance seems not applicable, this element is not analysed further. | Same as enrolment |
| **Trust factor Privacy:** | Since the compliance seems not applicable, this element is not analysed further. | Same as enrolment |
| **Trust factor Reputation:** | Since the compliance seems not applicable, this element is not analysed further. | Same as enrolment |

| 5 | **Policy:** ID-card | **Reference:** Article 4 Period of validity – Paragraph 1-3 |
|---|---|---|

1. Identity cards shall have a minimum period of validity of five years and a maximum period of validity of ten years.
2. By way of derogation from paragraph 1, Member States may provide for a period of validity of:
(a) less than five years, for identity cards issued to minors;
(b) in exceptional cases, less than five years, for identity cards issued to persons in special and limited circumstances and where their period of validity is limited in compliance with Union and national law;
(c) more than 10 years, for identity cards issued to persons aged 70 and above.
3. Member States shall issue an identity card having a validity of 12 months or less where it is temporarily physically impossible to take fingerprints of any of the fingers of the applicant.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | This element is analysed because supposedly paragraph 3 is within the scope of "biometric data on the ID-card" (being facial image and fingerprints). However this stipulation is only for the fingerprints. To analyse the purpose well, the whole article is analysed.<br><br>The article is about the period of validity and in paragraph 3 linked with the possibility (or not) of taking fingerprints. This could be extended to the possibility (or not) of taking facial images (referencing Article 3 Security standards/format/specifications – Paragraph 7 and Preamble 27).<br><br>Has thought been given to situations in which the facial image is also reason for exception? For example the mentioned very small babies that need to travel?! Maybe exceptions could be made for people not able to take pictures as well, just as they do for "not able to sign".<br><br>Compliance for the facial image is not an issue off course. | If there would be an exception for the validity period, it would be determined at the enrolment process. But then the ID-card could not be used for the authentication process.<br><br>Therefore not applicable |
| **Trust factor Usability:** | This element is about usability at the process of enrolment, trying to give a positive effect on special groups, younger children and other physically disabled persons. One thing is not mentioned here, that may be in the standards, is if person "temporarily" cannot capture biometric data. For example people who have a bruise in the face, or someone who is not in the exceptions in the standards, e.g. because of religious reasons (if the religion prohibits taking pictures, you cannot get an ID-card?) | Not applicable |
| **Trust factor Security:** | The security aspect is in the validity period itself. During the validity period the member state ensures the security of the issued card. As the validity period for minors is less, it could be discussed whether a member state should not trust minors with the card. Also the aging aspect of a minor (they change physical aspects during puberty) has a negative aspect on security, because it makes the photo not matching anymore. | Not applicable |
| **Trust factor Privacy:** | The reason for this stipulation is probably because of the privacy of the special groups. However this is not made explicit. The discussion could be that the policy can be made better if these aspects are made explicit. Explain in the policy why it is important. (Maybe I should look for it in the preambles, it is there in (27)! But then the discussion is | Not applicable |

| | | |
|---|---|---|
| | about whether the preambles form part of the policy or not…). And if it is because of other regulations (GDPR?) it could be made explicit as well. | |
| **Trust factor Reputation:** | The reputation of the process of taking fingerprints is in this element. It is "supposed" that smaller children should not, would not or can not take fingerprints. But this is not made explicit. The discussion could be that the policy can be made better if these aspects are made explicit. Explain in the policy why it is important. (Maybe it is in the preambles. But then the discussion is about whether the preambles form part of the policy or not…). | Not applicable |

| 6 | **Policy:** ID-card | **Reference:** Article 10 Collection of biometric identifiers – Paragraph 1-2 |
|---|---|---|

1. The biometric identifiers shall be collected solely by qualified and duly authorised staff designated by the authorities responsible for issuing identity cards or residence cards, for the purpose of being integrated into the highly secure storage medium provided for in Article 3(5) for identity cards and in Article 7(1) for residence cards. By way of derogation from the first sentence, fingerprints shall be collected solely by qualified and duly authorised staff of such authorities, except in the case of applications submitted to the diplomatic and consular authorities of the Member State. With a view to ensuring the consistency of biometric identifiers with the identity of the applicant, the applicant shall appear in person at least once during the issuance process for each application.
2. Member States shall ensure that appropriate and effective procedures for the collection of biometric identifiers are in place and that those procedures comply with the rights and principles set out in the Charter, the Convention for the Protection of Human Rights and Fundamental Freedoms and the United Nations Convention on the Rights of the Child. Where difficulties are encountered in the collection of biometric identifiers, Member States shall ensure that appropriate procedures are in place to respect the dignity of the person concerned.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | The whole procedure/technology for the enrolment, using the biometric data, shall only be used by "qualified and duly authorised staff designated by the authorities".<br>Except [fingerprints] in the case of applications submitted to the diplomatic and consular authorities of the Member State.<br>The applicant shall appear in person at least once during the issuance process for each application.<br>Procedures comply with the rights and principles set out in the Charter, the Convention for the Protection of Human Rights and Fundamental Freedoms and the United Nations Convention on the Rights of the Child. Where difficulties are encountered in the collection of biometric identifiers, Member States shall ensure that appropriate procedures are in place to respect the dignity of the person concerned.<br><br>In these two paragraphs several compliance elements are mentioned for the enrolment process. The important elements are the staff, the appearance in person and the compliance with international law/legislation, where is referred to the "dignity of the person".<br><br>The exception of diplomatic and consular authorities is put out of scope of this research, because they are not "regular" citizens.<br><br>A procedure of going to the municipality (at least once) and enrolling for the ID-card is compliant. Renewing the drivers license (not in scope) in the Netherlands, which is a procedure online with the handover of the document in person, seems also compliant.<br><br>The compliance with the mentioned international law/legislation is vague. How can compliance be determined? The term "dignity" is also vague. The discussion would be how dignity is involved in the process of enrolment of biometric data. | Not applicable |
| **Trust factor Usability:** | The usability aspect in this element lies within the question whether it is possible by the citizen to do the whole enrolment process.<br>By aspect: | Not applicable |

| | | |
|---|---|---|
| | To determine if the other party is "qualified and duly authorised staff". In the physical world the "duly authorised" is mostly accomplished by the uniform or some kind of badge that is used by the border patrol or police officer. Supposedly a municipal clerk who works at the municipality is also duly authorised, "designated by the authorities responsible for issuing identity cards or residence cards". The "qualified" part however is more difficult to determine by the citizen. If everything goes well and smooth, it is perceivable. If mistakes are made in the procedures of the enrolment process, the qualification of the clerk could be discussed.<br><br>The appearance in person might be difficult for people with a handicap and the way it is written "the applicant shall appear", seems to indicate that the applicant is responsible for appearing. What if he/she cannot? A better usability could be obtained by writing something like "the applicant shall be present" (which indicates a situation and not an action). Then possibly the clerk can go to the applicant (at its home) when necessary. It would improve the "dignity of the person" in such a situation. | |
| **Trust factor Security:** | The security aspect in this element is not found explicitly. However, the security aspect can be found when there is looked at the aspect of confidentiality. The enrolment process is supposed to be done face-to-face (at least once in the whole process), the citizen in front of the "qualified and duly authorised staff". Supposedly the information exchanged in this transaction, mostly by "handing over" the biometric data to the clerk, is confidential, although not every citizen might have enough trust to hand over the photo or give the fingerprints. Some parts of the enrolment process might be in the digital world, like taking the fingerprints or taking a digital(ised) photograph. It is impossible for a citizen to inspect this whole path of his biometric data, and even less doing this every time he does an enrolment (or application for it), and therefore the only way for the citizen is to have trust in security. The discussion could be whether this could be better integrated into the policy. | Not applicable |
| **Trust factor Privacy:** | The privacy aspect in this element is not found explicitly, but can be found in the *surroundings* of the enrolment process. For example the location where the enrolment process happens, like the municipality: is the process done in a private booth, a desk in a larger room etc. There might be other persons in the room (shoulder surfing) or even security camera's overlooking the whole process. The discussion would be whether these aspects are in the policy or some other policy. | Not applicable |
| **Trust factor Reputation:** | The reputation aspect in this element is not found explicitly, but can be found within the perception of the citizen about former experiences with the enrolment process.<br><br>The perception of the citizen about former experiences with "qualified and duly authorised staff" or by others. In the physical world this is seen by bad reputation of border control, police or government institutions like municipalities, even if this experience has nothing to do with the actual (technical) enrolment of the biometric data. Even if the enrolment always been "positive", some kind of distrust can be possible. So this is more about the reputation of the government. Also the reputation of the technical functioning of the equipment used for the enrolment can be at stake. Another reputation aspect is in the whole process, it might have a reputation of being too long, too cumbersome etc. | Not applicable |

| 7 | **Policy:** ID-card | **Reference:** Article 10 Collection of biometric identifiers – Paragraph 3 |
|---|---|---|

3. Other than where required for the purpose of processing in accordance with Union and national law, biometric identifiers stored for the purpose of personalisation of identity cards or residence documents shall be kept in a highly secure manner and only until the date of collection of the document and, in any case, no longer than 90 days from the date of issue. After this period, these biometric identifiers shall be immediately erased or destroyed.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | Important parts: shall be kept in a highly secure manner;<br>only until the date of collection of the document and, in any case, no longer than 90 days from the date of issue;<br>shall be immediately erased or destroyed [after this period].<br><br>The process of enrolment shall be compliant, but the difficulty within this element is that it is really about the process of storing data, *after* the enrolment. It makes it difficult to perceive how long the data are really kept and how the process of erasing or destroying takes place. Also the "highly secure manner" is not really determined within this policy, how the compliance can be accomplished is vague, and neither is the responsible organisation mentioned. Supposedly "the authorities responsible for issuing identity cards" are responsible.<br><br>The first part seems like an exception on the purpose of processing the data, so there might be (Union or national) law that has another purpose for storing the biometric identifiers? This leaves an opening for making a database with biometric identifiers, maybe for criminal investigation or national security intelligence. | Not applicable |
| **Trust factor Usability:** | There is not a real user part in this elements, at least it does not involve the citizen. The issuing authority (e.g. municipality) will be responsible for the storage of the data, so a municipal clerk might execute the storage of the data or a system. A usability aspect could be that the storage is implemented in such a way that the erase or destroy of the data cannot be forgotten "by accident". For a system that would be an automated task, for a clerk it would be a scheduled task to remove the physical data (e.g. photo). | Not applicable |
| **Trust factor Security:** | The term "highly secure" is very vague and not defined. Also the reason why it must be highly secure is not mentioned in this paragraph. Supposedly if digital data is used, the security of the storage system must be "high". Physical storage (e.g. photo) must also be secure, but it is not clear what kind of storage it would be. Maybe referring to (inter)national standards for data security could help. Also there is not mentioned who can have access to these data and for what reason. | Not applicable |
| **Trust factor Privacy:** | The term "highly secure" could be because of privacy as well. The discussion would be that it might be better to explicitly address the privacy aspect as reason of this stipulation. At least for privacy the purpose of storing the data is not clear, e.g. can identity cards be issued again with the same data if they are lost in the issuing process, or can users apply their rights of privacy to these biometric identifiers? | Not applicable |
| **Trust factor Reputation:** | The technology (product, brand) of storage are not really perceivable so for reputation there must be looked at "the authorities responsible for issuing identity cards" and its reputation for storage of data. With these biometric identifiers it might have the reputation of not storing (any) data in a highly secure manner. | Not applicable |

| 8 | **Policy:** ID-card | **Reference:** Article 11 Protection of personal data and liability – Paragraph 1-3 | |
|---|---|---|---|
| 1.Without prejudice to Regulation (EU) 2016/679, Member States shall ensure the security, integrity, authenticity and confidentiality of the data collected and stored for the purpose of this Regulation.<br>2.For the purpose of this Regulation, the authorities responsible for issuing identity cards and residence documents shall be considered as the controller referred to in Article 4(7) of Regulation (EU) 2016/679 and shall have responsibility for the processing of personal data.<br>3.Member States shall ensure that supervisory authorities can fully exercise their tasks as referred to in Regulation (EU) 2016/679, including access to all personal data and all necessary information as well as access to any premises or data processing equipment of the competent authorities. | | | |
| **Applicable to:** | | **enrolment** | **authentication** |
| **Compliance:** | | The reference to Regulation (EU) 2016/679 (GDPR) is made because of the personal (biometric) data in the process. It does not state that it should be compliant, it says "without prejudice [to the GDPR] shall ensure". It is not clear how compliance is accomplished, maybe it would have been better to just say that any solution for the data collection, storage and processing shall be compliant to the GDPR. For this research this is understood. | Same as enrolment, as the data stored (in the chip) also is being used for the authentication process. |
| **Trust factor Usability:** | | There is not a real user part in this elements, at least it does not involve the citizen. The issuing authority (e.g. municipality) will be responsible for the collection, storage and processing of the data with respect to the GDPR. Also the supervisory authority does not use the data.<br>Therefore not applicable. | Same as enrolment |
| **Trust factor Security:** | | This element is about security, mentioning other aspects of security: integrity, authenticity and confidentiality (of the data). Security is mentioned directly, what makes that it is not quite clear why the other aspects of security are mentioned, and the traditional "availability" within security is not. The authenticity (of data) seems new, normally authenticity is with persons (authentication) so it is assumed that the data really refers to an authentic person, which is a privacy aspect, just like confidentiality can be as well. | Same as enrolment |
| **Trust factor Privacy:** | | This element mentions the GDPR and some privacy aspects, but does not mention privacy explicitly. The authenticity (of data) seems a new term, normally authenticity is with persons (authentication) so it is assumed that the data really refers to an authentic person, which is a privacy aspect, just like confidentiality as well.<br><br>In paragraph 2 the controller is mentioned, referring to the GDPR and in paragraph 3 the supervisory authorities (of the GDPR). The discussion could be about how the GDPR must be incorporated into this policy, and then paragraph 2 and 3 could be excessive. So the controller and supervisory authorities should just be compliant with the GDPR. | Same as enrolment |
| **Trust factor Reputation:** | | The technology (product, brand) of storage are not really perceivable so for reputation there must be looked at "the authorities responsible for issuing identity cards" and its reputation for the processing of personal data, and the "supervisory authorities". With these biometric identifiers these authorities might have a bad reputation for the work with personal data in compliance with the GDPR. | Same as enrolment |

| 9 | **Policy:** ID-card | **Reference:** Article 11 Protection of personal data and liability – Paragraph 4 | |
|---|---|---|---|
| 4. Cooperation with external service providers shall not exclude any liability on the part of a Member State which may arise under Union or national law in respect of breaches of obligations with regard to personal data. | | | |
| **Applicable to:** | | **enrolment** | **authentication** |
| **Compliance:** | | This element seems unnecessary when the GDPR is referenced. As the controller of the data is an designated authority from the Member State, it is automatically liable in the GDPR. Therefore a reference to compliancy to the GDPR should be sufficient. | Same as enrolment |
| **Trust factor Usability:** | | Not applicable | Same as enrolment |
| **Trust factor Security:** | | Not applicable | Same as enrolment |
| **Trust factor Privacy:** | | The liability of "breaches of obligations with regard to personal data" seems to be a privacy aspect, new to this research. However it should be in the GDPR, so the discussion could be that it is better to refer to the GDPR. | Same as enrolment |
| **Trust factor Reputation:** | | The technology (product, brand) of storage are not really perceivable so for reputation there must be looked at "the authorities responsible for issuing identity cards" and its reputation for the processing of personal data, and the "supervisory authorities". With these biometric identifiers these authorities might have a bad reputation for the work with personal data in compliance with the GDPR. | Same as enrolment |

| **10** | **Policy:** ID-card | **Reference:** Article 11 Protection of personal data and liability – Paragraph 5 | |
|---|---|---|---|
| 5. Information in machine-readable form shall only be included in an identity card or residence document in accordance with this Regulation and the national law of the issuing Member State. | | | |
| **Applicable to:** | | **enrolment** | **authentication** |
| **Compliance:** | | This paragraph seems a little out of context with the rest of the article 11, which is about GDPR / Privacy. The definition of "information in machine-readable form" is not found, other than the MRZ in article 3 paragraph 1. The whole information in the contactless chip, which is readable by NFC technology might be in scope of this element as well.<br><br>The stipulation is "shall only be included in an identity card or residence document". Looking at the scope in article 2, there are 3 types of documents in scope and b) being "registration certificates issued in accordance with Article 8 of Directive 2004/38/EC". So this paragraph only applies to registration certificates, which apparently cannot hold machine readable data (Why not? A QR-code maybe?).<br><br>The discussion could be that this paragraph should be only about the registration certificates, and could be better transferred to article 6, (f) "the information to be included on registration certificates and documents certifying permanent residence, issued in accordance with Articles 8 and 19 of Directive 2004/38/EC, respectively;".<br>Therefore not applicable | Same as enrolment, Not applicable |
| **Trust factor Usability:** | | Not applicable | Not applicable |
| **Trust factor Security:** | | Not applicable | Not applicable |
| **Trust factor Privacy:** | | Not applicable | Not applicable |
| **Trust factor Reputation:** | | Not applicable | Not applicable |

| **11** | **Policy:** ID-card | **Reference:** Article 11 Protection of personal data and liability – Paragraph 6 |
|---|---|---|

Biometric data stored in the storage medium of identity cards and residence documents shall only be used in accordance with Union and national law, by the duly authorised staff of competent national authorities and Union agencies, for the purpose of verifying:

(a) the authenticity of the identity card or residence document;

(b) the identity of the holder by means of directly available comparable features where the identity card or residence document is required to be produced by law.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | Not applicable | The solution that authenticates using the biometric data, shall only be used by "duly authorised staff". Taking this literally, this would mean that only a person could do the verification mentioned in (a) and (b), and not a machine or technology. However, any technical solution, which could be seen as a procedure that involves technology, should only be *operated by* duly authorised staff. In physical identity verification this usually is compliant when staff like a border patrol or police officer does the verification with some device the officer operates. In digital identity verification the whole procedure is through/over the Internet, and without a person on the other side, only a machine, so compliance is only possible if the solution acts *on behalf of* duly authorised staff. This compliance could be discussed. An additional discussion could be raised if *supervision by* duly authorised staff should also be necessary, which might be problematic in the digital world.<br><br>The last part of (b), "where the identity card … is required to be produced by law", however indicates that this stipulation is only true if the purpose of verifying is required by law. This "required identity verification", in the physical world seen with border and police control, might have its digital equivalent, but has not been stipulated in this policy. So the question remains when identity verification over the Internet is required by law. Answering this question would require further research but for this research the assumption is made that for eGovernment the identity verification indeed is required. |
| **Trust factor Usability:** | Not applicable | The usability aspect in this element lies within the question whether it is possible by the citizen to determine if the other party is "duly authorised staff". In the physical world this is mostly accomplished by the uniform or some kind of badge that is used by the border patrol or police officer. In the digital world this positive trust effect is mostly accomplished by using website certificates and trust seals, as stipulated in the eIDAS policy. However, these tools can be faked and spoofed or even be not familiar to the citizen, resulting in a negative effect on trust. |
| **Trust factor Security:** | Not applicable | The security aspect in this element is not found explicitly. However, the security aspect can be found when there is looked at the aspect of confidentiality. In the physical world, the identity verification is supposed to be done face-to-face, the citizen in front of the "duly authorised staff". Supposedly the information exchanged in this transaction, mostly by handing over the physical identity card to the officer to by read by the device, is confidential, although not every citizen might have enough trust to hand over the identity card and only want to show it or to inspect the device first. In the digital world, when reading the identity card with your own smartphone, there is a lot more to distrust. In fact there is no actual handover of the identity card but the data confidentiality can already be breached in the NFC part, then within the smartphone and then within the communication over the Internet. It is impossible for a citizen to inspect this whole path of his biometric data, and even less doing this every time he uses the solution, and therefore the only way for the citizen is to have trust in security. The discussion could be whether this could be better integrated into the policy. |

| | | |
|---|---|---|
| **Trust factor Privacy:** | Not applicable | The privacy aspect in this element is in the *purpose* of the usage of the biometric data, which is explicitly defined by (a) and (b). Citizen can trust in their privacy if any usage only adheres to this purpose. However, with the NFC technology it is possible to "accidentally" read the chip in the identity card, which could lead to privacy problems. Similar problems are seen with the NFC-enabled banking cards nowadays. Citizens could protect the privacy of their data in the identity card by using NFC blocking wallets or card holders, which is actually a symbol of negative trust towards the used technology.<br><br>A question that could be raised is whether a voluntarily usage of the biometric data, with explicit consent of the citizen, is allowed and could be used for other procedures, like for example handing in a digital photo for a user profile or other private use. This would be like adding option (c) to this paragraph or have an exception, which would alter the policy. The discussion would be about ownership of data, freedom of data and thus lead to a discussion about the so called "self sovereign identity", which is beyond the scope of this research. |
| **Trust factor Reputation:** | Not applicable | The reputation aspect in this element is not found explicitly, but can be found within the perception of the citizen about former experiences with "duly authorised staff" or by others. In the physical world this is seen by bad reputation of border control or police, even if this experience has nothing to do with the actual (technical) verification of the identity. Even if the identity verification with the identity card has always been "positive" (a match), some kind of distrust can be possible. In the digital world this distrust in "duly authorised staff" might be absent because of the technology is "acting on behalf", leading to the earlier mentioned "scientific truth". The discussion would be more about whether the solution as a whole is "duly authorised", and the (technical) manufacturer, the brand or the owner of the solution (supposedly the government) could have a bad reputation. |

| **12** | **Policy:** ICAO | **Reference:** 2.1 Conformance to Doc 9303 | |
|---|---|---|---|
| An electronic MRTD (eMRTD) SHALL conform in all respects to the specifications provided in Doc 9303. | | | |
| **Applicable to:** | | **enrolment** | **authentication** |
| **Compliance:** | | An eMRTD, which is a special form of MRTD, shall "conform" to the whole (set of) ICAO Document 9303.<br>https://www.icao.int/publications/pages/publication.aspx?docnum=9303<br><br>The ID-card shall be compliant, but the discussion could be how compliance to a standard is measured and by whom, what authority. Also the supervision authority for compliance to standards is not defined. | Same as enrolment |
| **Trust factor Usability:** | | Not applicable, there is no usability aspect in this element | Same as enrolment |
| **Trust factor Security:** | | Not applicable, there is no security aspect in this element | Same as enrolment |
| **Trust factor Privacy:** | | Not applicable, there is no privacy aspect in this element | Same as enrolment |
| **Trust factor Reputation:** | | The eMRTD is not a technology that seems not be known widely, nor the standards on it that are held by ICAO. Even the ICAO as organisation is not very known, although almost every citizen in the world has to do with its standards when travelling by air. Therefore it is not likely that reputation has an negative effect on the eMRTD itself. | Same as enrolment |

| **13** | **Policy:** ICAO | **Reference:** 2.2 Validity Period for an eMRTD | |
|---|---|---|---|
| The validity period of an eMRTD is at the discretion of the issuing State or organization; however, in consideration of the limited durability of documents and the changing appearance of the document holder over time, a validity period of not more than ten years is RECOMMENDED. One MAY wish to consider a shorter period to enable the progressive upgrading of the eMRTD as the technology evolves. | | | |
| **Applicable to:** | | **enrolment** | **authentication** |
| **Compliance:** | | This element is only a recommendation, so compliance is *not an issue*. It contains some interesting aspects, for which it is analysed further. | The validity period is set in the enrolment / issuing phase, so *not applicable*. However, it contains interesting aspects, for which it is analysed further. |
| **Trust factor Usability:** | | There are usability aspects in this element, that can determine the right validity period for an eMRTD.<br>- limited durability of documents (wear and tear)<br>- changing appearance of the document holder over time (aging)<br>- progressive upgrading of the eMRTD as the technology evolves (phasing out of older technology) | Although the validity period is set in the enrolment / issuing phase, problems with the usability aspects will arise in the authentication phase. So usability is an important aspect to determine the right validity period for an eMRTD. |
| **Trust factor Security:** | | The progressive upgrading / phasing out of technology is a security aspect. Old technology probably has security issues. | Although the validity period is set in the enrolment / issuing phase, problems with the security will arise in the authentication phase. So security is an important aspect to determine the right validity period for an eMRTD. |
| **Trust factor Privacy:** | | The progressive upgrading / phasing out of technology is a privacy aspect. Old technology probably has issues of keeping the personal data safe. | Although the validity period is set in the enrolment / issuing phase, problems with the privacy will arise in the authentication phase. So privacy is an important aspect to determine the right validity period for an eMRTD. |
| **Trust factor Reputation:** | | The validity period might have reputation aspects. A (too) long validity period can be negative (it always breaks before the validity period is over) but also a too short validity period can have citizen wonder why they have to renew the card so often (is it bad?) | Same as enrolment |

| **14** | **Policy:** ICAO | **Reference:** 3.1 ICAO Vision on biometrics |
|---|---|---|

Doc 9303 considers only three types of biometric identification systems. With respect to the storage of these three biometric features in the contactless IC of an eMRTD, the issuing State or organization SHALL conform to the relevant international standard.
The types of biometrics are:
• facial recognition – REQUIRED;
• fingerprint recognition – OPTIONAL;
• iris recognition – OPTIONAL.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | The ID-card is compliant to the requirement of having facial recognition in an eMRTD. | Same as enrolment |
| **Trust factor Usability:** | The usability aspect is only indirect: the facial recognition is the most direct and usable form of biometric identification, as in the physical world, where it can be done by almost everyone. | Same as enrolment |
| **Trust factor Security:** | Not applicable, there is no security aspect | Not applicable, there is no security aspect |
| **Trust factor Privacy:** | Not applicable, there is no privacy aspect | Not applicable, there is no privacy aspect |
| **Trust factor Reputation:** | The eMRTD is not a technology that seems not be known widely, nor the standards on it that are held by ICAO. Even the ICAO as organization is not very known, although almost every citizen in the world has to do with its standards when travelling by air. Therefore it is not likely that reputation has an negative effect on the eMRTD itself. | Same as enrolment |

| **15** | **Policy:** ICAO | **Reference:** 3.2 Key Considerations |
|---|---|---|

In specifying biometric applications for eMRTDs, key considerations are:
• Global Interoperability — the crucial need to specify a system for deployment to be used in a universally interoperable manner;
• Uniformity — the need to minimize via specific standard setting, to the extent practical, the different solution variations that may potentially be deployed by issuing States or organizations;
• Technical Reliability — the need to provide guidelines and parameters to ensure issuing States or organizations deploy technologies that have been proven to provide a high level of confidence from an
identity confirmation viewpoint; and that States or organizations reading data encoded by other issuing States or organizations can be sure that the data supplied to them are of sufficient quality and integrity to enable accurate verification in their own system;
• Practicality — the need to ensure that recommended standards can be made operational and implemented by States or organizations without their having to introduce a plethora of disparate systems and equipment to ensure they meet all possible variations and interpretations of the standards;
• Durability — the requirement that the systems introduced will last the recommended maximum 10-year life of a travel document, and that future updates will be backward compatible.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | This element is only a recommendation, so compliance is *not an issue*. It contains some interesting aspects, for which it is analysed further. | Same as enrolment |
| **Trust factor Usability:** | The considerations are aspects that adhere mostly to usability of the eMRTD. | Same as enrolment |
| **Trust factor Security:** | The aspect of *technical reliability* is also a security aspect:<br>- deploy technologies that have been proven to provide a high level of confidence,<br>- the data supplied […] are of sufficient quality and integrity to enable accurate verification | Same as enrolment |
| **Trust factor Privacy:** | Not applicable, there are no privacy aspects. | Same as enrolment (Not applicable) |
| **Trust factor Reputation:** | The eMRTD is not a technology that seems not be known widely, nor the standards on it that are held by ICAO. Even the ICAO as organisation is not very known, although almost every citizen in the world has to do with its standards when travelling by air. Therefore it is not likely that reputation has an negative effect on the eMRTD itself. | Same as enrolment |

| **16** | **Policy:** ICAO | **Reference:** 3.5 Constraints on Biometric Solutions | |
|---|---|---|---|
| It is recognized that implementation of most biometrics technologies is subject to further development. Given the rapidity of technological change, any specifications (including those herein) must allow for, and recognize there will be, changes resulting from technology improvements. The biometrics information stored on travel documents shall comply with any national data protection laws or privacy laws of the issuing State or organization. | | | |
| **Applicable to:** | | **enrolment** | **authentication** |
| **Compliance:** | | Any specifications (including those herein) must allow for, and recognize there will be, changes resulting from technology improvements. *How* this compliance should be accomplished is a discussion point (regulation vs. standards). | Same as enrolment |
| **Trust factor Usability:** | | The usability aspect is indirect, implementation of most biometrics technologies is subject to further development | Same as enrolment |
| **Trust factor Security:** | | The security aspect is indirect, given the rapidity of technological change | Same as enrolment |
| **Trust factor Privacy:** | | Privacy is in this element<br>The biometrics information stored on travel documents shall comply with any national *data protection laws or privacy laws* of the issuing State or organisation. | Same as enrolment |
| **Trust factor Reputation:** | | There could be a reputation aspect in biometric technologies as a whole. People could be reluctant to technology in general. | Same as enrolment |

| **17** | **Policy:** ICAO | **Reference:** 5.3 Security and Privacy of the Stored Data |
|---|---|---|

Both the issuing and any receiving States or organizations need to be satisfied that the data stored on the contactless IC have not been altered since they were recorded at the time of issue of the document. In addition, the privacy laws or practice of the issuing State or organization may require that the data cannot be accessed except by an authorized person or organization. Accordingly ICAO has developed specifications in Doc 9303-11 and Doc 9303-12 regarding the application and usage of modern encryption techniques, particularly Public Key Infrastructure (PKI) schemes, which MUST be used by issuing States or organizations in their Machine Readable Travel Documents made in accordance with Doc 9303.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | This element has several parts for compliance:<br>- *need to be satisfied that* the data […] *have not been altered* since […] the time of issue of the document.<br>- *may require that* the data *cannot be accessed* except by an authorized person or organization<br>- *specifications* in Doc 9303-11 / 12 […] *must be used* […] in […] MRTDs<br><br>So for compliance also other parts of the ICAO Document 9303 are needed. In this research this is not done but it is left for further research.<br>The ID-card is to be compliant (“shall be based on”). | Although the technology and the compliance is set in the enrolment / issuing phase, problems with the alteration of data or unauthorised access will arise in the authentication phase.<br>Therefore same as enrolment. |
| **Trust factor Usability:** | The usability aspect in the enrolment phase is that the (facial image) data is stored exactly as the image was captured, and no alteration has taken place. Signing of data is a solution for this and is probably in the referenced ICAO Docs. Loss of quality of the image in the enrolment phase might still be an issue. | The usability aspect in the authentication phase is that, if the (facial image) data is altered, it probably will not function well anymore. The mechanism for checking alteration (probably signing) can have usability aspects. |
| **Trust factor Security:** | The security aspect is in the integrity and confidentiality of the data during its whole existence. Also the usage of encryption techniques is a security aspect. | The security aspect is in the integrity and confidentiality of the data during its whole existence. Also the usage of encryption techniques is a security aspect. |
| **Trust factor Privacy:** | Privacy is in this element by mentioning privacy laws or practice and is applied to the confidentiality of the data. | Privacy is in this element by mentioning privacy laws or practice and is applied to the confidentiality of the data. |
| **Trust factor Reputation:** | The technology (product, brand) of the contactless IC are not really perceivable so for reputation there must be looked at “the issuing State or organization” and its reputation for the processing of personal data. With these biometric identifiers these authorities might have a bad reputation for the work with personal data in compliance with the privacy laws or practice. | Same as enrolment |

| **18** | **Policy:** ICAO | **Reference:** 7. References (normative) |
|---|---|---|

[A list of references, among which in scope:]
ISO/IEC 14443-2:2016, Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 2: Radio frequency power and signal interface.
ISO/IEC 14443-3:2016 (corrected version 2016-09-01), Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and anticollision
ISO/IEC 14443-4:2016, Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol
ISO/IEC 19794-5:2005, Information technology — Biometric data interchange formats — Part 5: Face image data
ISO/IEC 39794-5, Information technology — Extensible biometric data interchange formats — Part 5: Face image data

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | For compliance all the referenced ISO standards are needed, since they are “normative" according to ICAO. In this research this is not done but it is left for further research. *How* this compliance should be accomplished is a discussion point (regulation vs. standards).<br>The ID-card is to be compliant (“shall be based on”).<br><br>The discussion could be why assumably relevant ISO standards are not mentioned:<br>ISO 24745: Biometric information protection<br>ISO 30107: Biometric presentation attack detection | Same as enrolment |
| **Trust factor Usability:** | Some of the referenced ISO standards seem to have usability aspects (according to the titles). In this research this is left for further research. | Same as enrolment |
| **Trust factor Security:** | Some of the referenced ISO standards seem to have security aspects (according to the titles). In this research this is left for further research. | Same as enrolment |
| **Trust factor Privacy:** | Some of the referenced ISO standards seem to have privacy aspects (according to the titles). In this research this is left for further research. | Same as enrolment |
| **Trust factor Reputation:** | The reputation aspect could be in the use of standards and how to verify these standards? Or is it just about reputation of or trust in the organisations? (So the EU trusts the ICAO, the ICAO trusts the ISO, etc.) | Same as enrolment |

| **19** | **Policy:** eIDAS | **Reference:** Article 5 Data processing and protection | |
|---|---|---|---|
| 1. Processing of personal data shall be carried out in accordance with Directive 95/46/EC. | | | |
| **Applicable to:** | | **enrolment** | **authentication** |
| **Compliance:** | | The reference of this element is to the predecessor of the GDPR, but in effect it is a reference to the GDPR. Somehow it is a little vague with "shall be *carried out in accordance with*" instead of "shall be *compliant with*". However, compliance with the GDPR should be the purpose for the proposed solution. | Same as enrolment. |
| **Trust factor Usability:** | | There is no usability aspect in this element, so not applicable. | Same as enrolment. |
| **Trust factor Security:** | | There is no security aspect in this element, so not applicable. | Same as enrolment. |
| **Trust factor Privacy:** | | The whole article is about protecting the privacy of personal data. | Same as enrolment. |
| **Trust factor Reputation:** | | There is no reputation aspect in this element, so not applicable. | Same as enrolment. |

| **20** | **Policy:** eIDAS | **Reference:** Article 6 Mutual recognition |
|---|---|---|

1. When an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector body online in one Member State, the electronic identification means issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that service online, provided that the following conditions are met:
(a) the electronic identification means is issued under an electronic identification scheme that is included in the list published by the Commission pursuant to Article 9;
(b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first Member State, provided that the assurance level of that electronic identification means corresponds to the assurance level substantial or high;
(c) the relevant public sector body uses the assurance level substantial or high in relation to accessing that service online.
Such recognition shall take place no later than 12 months after the Commission publishes the list referred to in point (a) of the first subparagraph.
2. An electronic identification means which is issued under an electronic identification scheme included in the list published by the Commission pursuant to Article 9 and which corresponds to the assurance level low may be recognised by public sector bodies for the purposes of cross-border authentication for the service provided online by those bodies.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | This element sets the rules for mutual recognition of eID solutions between Member States.<br>The first paragraph mentions two important options (for the "shall be recognised"):<br>- when authentication is required under national law, or<br>- by administrative practice to access a service provided by a public sector body online<br>Then the conditions (a), (b) and (c) should be met.<br>(a) is about the notification of article 9<br>(b) is about the minimum level of substantial or high<br>(c) is about the public sector body using level substantial or high<br>The second paragraph makes the whole article optional for level low.<br><br>So recognition is mandatory for levels substantial and high for an online service of a public sector body. It is optional for level low. | Same as enrolment. |
| **Trust factor Usability:** | Although recognition is not very usable, its goal is supposed to make the eID solution usable for cross-border authentication. How this is accomplished, is not mentioned in this article. Probably it will be in the cooperation and interoperability of article 12. | Same as enrolment. |
| **Trust factor Security:** | There is no security aspect in this element, so not applicable. | Same as enrolment. |
| **Trust factor Privacy:** | There is no privacy aspect in this element, so not applicable. | Same as enrolment. |
| **Trust factor Reputation:** | Recognition can be seen as a reputation aspect. One Member State recognizes an eID solution of another, it assumes a good reputation. | Same as enrolment. |

| 21 | **Policy:** eIDAS | **Reference:** Article 7 Eligibility for notification of electronic identification schemes |
|---|---|---|

An electronic identification scheme shall be eligible for notification pursuant to Article 9(1) provided that all of the following conditions are met:
(a) the electronic identification means under the electronic identification scheme are issued:
(i) by the notifying Member State;
(ii) under a mandate from the notifying Member State; or
(iii) independently of the notifying Member State and are recognised by that Member State;
(b) the electronic identification means under the electronic identification scheme can be used to access at least one service which is provided by a public sector body and which requires electronic identification in the notifying Member State;
(c) the electronic identification scheme and the electronic identification means issued thereunder meet the requirements of at least one of the assurance levels set out in the implementing act referred to in Article 8(3);
(d) the notifying Member State ensures that the person identification data uniquely representing the person in question is attributed, in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3), to the natural or legal person referred to in point 1 of Article 3 at the time the electronic identification means under that scheme is issued;
(e) the party issuing the electronic identification means under that scheme ensures that the electronic identification means is attributed to the person referred to in point (d) of this Article in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3);
(f) the notifying Member State ensures the availability of authentication online, so that any relying party established in the territory of another Member State is able to confirm the person identification data received in electronic form. For relying parties other than public sector bodies the notifying Member State may define terms of access to that authentication. The cross-border authentication shall be provided free of charge when it is carried out in relation to a service online provided by a public sector body. Member States shall not impose any specific disproportionate technical requirements on relying parties intending to carry out such authentication, where such requirements prevent or significantly impede the interoperability of the notified electronic identification schemes;
(g) at least six months prior to the notification pursuant to Article 9(1), the notifying Member State provides the other Member States for the purposes of the obligation under Article 12(5) a description of that scheme in accordance with the procedural arrangements established by the implementing acts referred to in Article 12(7);
(h) the electronic identification scheme meets the requirements set out in the implementing act referred to in Article 12(8).

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | This element sets the rules for notification of eID solutions.<br>Part (a) stipulates that the eID solution is issued by, under a mandate of or recognised by a Member State. For the proposed solution (the ID-card) it is compliant<br>Part (b) mentions the usability for at least one online service of a public sector body, alike article 6. The proposed solution is for eGovernment, so compliance is no problem.<br>Parts (c), (d) and (e) mention the corresponding assurance level. Compliance to the assurance levels is analysed later.<br>Part (f) ensures availability of online cross-border authentication, by confirmation of the person identification data, being free of charge for a public sector body, and being interoperable (“not … any specific disproportionate technical requirements”).<br>Parts (g) and (h) refer further to article 12 for cooperation and interoperability.<br>These aspects of cooperation and interoperability are very important for the proposed eID solution. | Same as enrolment. |

| | | |
|---|---|---|
| **Trust factor Usability:** | Although notification is not very usable, its goal is supposed to make the eID solution usable for cross-border authentication. How this is accomplished, is not mentioned in this article. Probably it will be in the cooperation and interoperability of article 12. Cooperation and interoperability are usability aspects. | Same as enrolment. |
| **Trust factor Security:** | The security aspect is indirectly in the references to the assurance levels. | Same as enrolment. |
| **Trust factor Privacy:** | The privacy aspect is indirectly in the references to the assurance levels. | Same as enrolment. |
| **Trust factor Reputation:** | Notification can be seen as a reputation aspect. The EU notifies an eID solution of a Member State; the EU gives a (good) reputation. | Same as enrolment. |

| **22** | **Policy:** eIDAS | **Reference:** Article 8 Assurance levels of electronic identification schemes |
|---|---|---|

1. An electronic identification scheme notified pursuant to Article 9(1) shall specify assurance levels low, substantial and/or high for electronic identification means issued under that scheme.
2. The assurance levels low, substantial and high shall meet respectively the following criteria:
(a) assurance level low shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity;
(b) assurance level substantial shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;
(c) assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | This element specifies the assurance levels of low, substantial and high. The differences between the levels seem vague, being "to decrease the risk of", "to decrease substantially the risk of" and "to prevent" *misuse or alteration of the identity* respectively.<br>The words used, *assurance* and *confidence* refer to trust, so the discussion could be that a / the goal of eIDAS is to seek trust in eID solutions.<br>Compliance to the assurance levels is analysed later. | Same as enrolment. |
| **Trust factor Usability:** | There is a negative usability aspect in this element, namely the *misuse or alteration of the identity*. Supposedly it would make the identity less usable for the intended user. | Same as enrolment. |
| **Trust factor Security:** | The security aspect is indirectly in the references to the assurance levels. | Same as enrolment. |
| **Trust factor Privacy:** | The privacy aspect is indirectly in the references to the assurance levels. | Same as enrolment. |
| **Trust factor Reputation:** | The assurance levels itself are a reputation aspect. When a certain assurance level is met, the eID solution has a good reputation for that level, with limited, substantial or higher degree of confidence (trust). | Same as enrolment. |

| **23** | **Policy:** eIDAS | **Reference:** Article 9 Notification |
|---|---|---|

1. The notifying Member State shall notify to the Commission the following information and, without undue delay, any subsequent changes thereto:
(a) a description of the electronic identification scheme, including its assurance levels and the issuer or issuers of electronic identification means under the scheme;
(b) the applicable supervisory regime and information on the liability regime with respect to the following:
(i) the party issuing the electronic identification means; and
(ii) the party operating the authentication procedure;
(c) the authority or authorities responsible for the electronic identification scheme;
(d) information on the entity or entities which manage the registration of the unique person identification data;
(e) a description of how the requirements set out in the implementing acts referred to in Article 12(8) are met;
(f) a description of the authentication referred to in point (f) of Article 7;
(g) arrangements for suspension or revocation of either the notified electronic identification scheme or authentication or the compromised parts concerned.
2. One year from the date of application of the implementing acts referred to in Articles 8(3) and 12(8), the Commission shall publish in the Official Journal of the European Union a list of the electronic identification schemes which were notified pursuant to paragraph 1 of this Article and the basic information thereon.
3. If the Commission receives a notification after the expiry of the period referred to in paragraph 2, it shall publish in the Official Journal of the European Union the amendments to the list referred to in paragraph 2 within two months from the date of receipt of that notification.
4. A Member State may submit to the Commission a request to remove an electronic identification scheme notified by that Member State from the list referred to in paragraph 2. The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list within one month from the date of receipt of the Member State's request.
5. The Commission may, by means of implementing acts, define the circumstances, formats and procedures of notifications under paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | This element is analysed to have more information about the notification process and its trust factor reputation. Compliance to this element is not an issue for the proposed solution. | Same as enrolment. |
| **Trust factor Usability:** | The usability aspect is in the information that is in the notification, especially in 1.(a)., the description of the eID solution and its assurance levels. Also elements 1.(e) and (f) are usability aspects, a citizen can read how the eID solution should or can be used. | Same as enrolment. |
| **Trust factor Security:** | The security aspect is in the information that is in the notification, especially in 1.(a)., which mentions the assurance levels. | Same as enrolment. |
| **Trust factor Privacy:** | The privacy aspect is in the information that is in the notification, especially in 1.(a)., which mentions the assurance levels. Also 1.(b) and 1.(c) contain important information about the privacy of personal data, because of the supervision, liability and responsibility for the eID solution. | Same as enrolment. |
| **Trust factor Reputation:** | The reputation aspect is in the notification itself, which is about information about an eID solution that is officially published. It is like an official review of the EU Commission. So the conclusion can be that reputation is about public or published information. | Same as enrolment. |

| **24** | **Policy:** eIDAS | **Reference:** Article 10 Security breach |
|---|---|---|

1. Where either the electronic identification scheme notified pursuant to Article 9(1) or the authentication referred to in point (f) of Article 7 is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission.
2. When the breach or compromise referred to in paragraph 1 is remedied, the notifying Member State shall re- establish the cross-border authentication and shall inform other Member States and the Commission without undue delay.
3. If the breach or compromise referred to in paragraph 1 is not remedied within three months of the suspension or revocation, the notifying Member State shall notify other Member States and the Commission of the withdrawal of the electronic identification scheme.
The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list referred to in Article 9(2) without undue delay.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | This element is analysed because of the explicit security aspect. Supposedly for the proposed eID solution, a suitable procedure for security breaches can be designed and compliance is then of no issue. | Same as enrolment. |
| **Trust factor Usability:** | There is no usability aspect in this element, so not applicable. | Same as enrolment. |
| **Trust factor Security:** | The security aspect is in the (possible) security breach or compromise of the eID solution. It is a negative security effect but by having a procedure for suspending or revoking and for informing concerned parties, the negative effect might be smaller. | Same as enrolment. |
| **Trust factor Privacy:** | There is no privacy aspect in this element, so not applicable. | Same as enrolment. |
| **Trust factor Reputation:** | The reputation aspect is in the informing other Member States and the Commission. It is like doing an official publication about the security breach. It might have a negative effect on reputation if security breaches happen a lot. | Same as enrolment. |

| **25** | **Policy:** eIDAS | **Reference:** Article 11 Liability | |
|---|---|---|---|
| 1. The notifying Member State shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with its obligations under points (d) and (f) of Article 7 in a cross-border transaction.<br>2. The party issuing the electronic identification means shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligation referred to in point (e) of Article 7 in a cross- border transaction.<br>3. The party operating the authentication procedure shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to ensure the correct operation of the authentication referred to in point (f) of Article 7 in a cross-border transaction. | | | |
| **Applicable to:** | | **enrolment** | **authentication** |
| **Compliance:** | | This element is analysed because of the explicit liability that is pursued by the regulation. Compliance for the proposed eID solution is to be designed in some liability procedure. But the discussion could be about how liability can be effective in an international / EU context. | Same as enrolment. |
| **Trust factor Usability:** | | There is no usability aspect in this element, so not applicable. | Same as enrolment. |
| **Trust factor Security:** | | There is no usability aspect in this element, so not applicable. | Same as enrolment. |
| **Trust factor Privacy:** | | There is no usability aspect in this element, so not applicable. | Same as enrolment. |
| **Trust factor Reputation:** | | Liability seems to be a reputation aspect, because it is about “damage caused intentionally or negligently to any natural or legal person”. Whenever there is a liability case, which is probably in the public domain, it is bad for reputation. | Same as enrolment. |

| **26** | **Policy:** eIDAS | **Reference:** Article 12 Cooperation and interoperability |
|---|---|---|

1. The national electronic identification schemes notified pursuant to Article 9(1) shall be interoperable.
2. For the purposes of paragraph 1, an interoperability framework shall be established.
3. The interoperability framework shall meet the following criteria:
(a) it aims to be technology neutral and does not discriminate between any specific national technical solutions for electronic identification within a Member State;
(b) it follows European and international standards, where possible;
(c) it facilitates the implementation of the principle of privacy by design; and
(d) it ensures that personal data is processed in accordance with Directive 95/46/EC.
4. The interoperability framework shall consist of:
(a) a reference to minimum technical requirements related to the assurance levels under Article 8;
(b) a mapping of national assurance levels of notified electronic identification schemes to the assurance levels under Article 8;
(c) a reference to minimum technical requirements for interoperability;
(d) a reference to a minimum set of person identification data uniquely representing a natural or legal person, which is available from electronic identification schemes;
(e) rules of procedure;
(f) arrangements for dispute resolution; and
(g) common operational security standards.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | This element is analysed because of several other article referring to it. Some important aspect about the interoperability are mentioned.<br>The interoperability must be *technology neutral* [3.(a)]. However it is unclear how compliance to technology neutral can be met. The following of European and international standards, where possible [3.(b)], does not specify its compliance either. The referral to privacy in 3.(c) and 3.(d) is direct, but vague in terms of “facilitates” and “in accordance with”. The specifications of the interoperability in paragraph 4 is not easily interpreted for compliance. Supposedly, the proposed solution that uses the standardized ID-card, should be compliant. | Same as enrolment. |
| **Trust factor Usability:** | Interoperability seems to be a usability aspect. When the eID solution is interoperable between Member States, it can be used in all Member States in the same way. | Same as enrolment. |
| **Trust factor Security:** | The security aspect is in the standards, mentioned in 3.(b) and 4.(g). | Same as enrolment. |
| **Trust factor Privacy:** | The privacy aspect is explicitly in 3.(c) and 3.(d), but vague in terms of “facilitates” and “in accordance with”. | Same as enrolment. |
| **Trust factor Reputation:** | The reputation aspect can be found in 4.(f). Dispute resolution, just like liability, can have a negative effect on reputation. | Same as enrolment. |

| **27** | **Policy:** LoA's | **Reference:** 2.1. Enrolment – 2.1.1. Application and registration | |
|---|---|---|---|
| *Low / Substantial / High*<br>1. Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means.<br>2. Ensure the applicant is aware of recommended security precautions related to the electronic identification means.<br>3. Collect the relevant identity data required for identity proofing and verification. | | | |
| **Applicable to:** | | **enrolment** | **authentication** |
| **Compliance:** | | All the assurance levels must be compliant to this element.<br>The first part is awareness of the terms and conditions. So in the application process, the (future) use of the biometric data for electronic identification (authentication) must be set. There is no indication of how this should be accomplished, but an implementation could be by explicitly accepting the terms and conditions by the applicant, by placing a signature.<br>The second part is awareness about the security measures to take by the applicant. This awareness could be about the biometric data (photo) in the chip, preventing third parties to read the chip or using NFC-blocking wallets.<br>The third part is just about the process of enrolment and the ID-card is supposed to be compliant. | Not applicable |
| **Trust factor Usability:** | | Terms and conditions (1) are a usability aspect, as they are related to the use of the biometric data. However, mostly the terms and conditions have a limiting effect on usability, also because the applicant might find it difficult to read and accept the terms and conditions. So the discussion could be how terms and conditions should be presented (made aware) to the applicant.<br>Also the security precautions (2) have a usability aspect, because mostly security precautions make technology less usable. So also the framing of security should be done in a way that trust is enhanced.<br>The collection of the biometric data is the usage itself, and the applicant should be able to do this process of enrolment. | Not applicable |
| **Trust factor Security:** | | The security aspect is in the awareness of security precautions (2). If there are many security precautions, there could be a negative effect on trust, so framing the security precautions in a positive way could be positive for trust as well. So the discussion could be how awareness about security (of the specific solution) could be done.<br>A security aspect that seems to be forgotten is the security of the collection of the data (3), so *how* it is done in a secure way. | Not applicable |
| **Trust factor Privacy:** | | There seems no privacy aspect in this element. The discussion could be of *how* the process of collecting the data (3) could be done in a privacy enhancing way, for example in the setup for taking the photo (a personal booth etc.). | Not applicable |
| **Trust factor Reputation:** | | There seems no reputation aspect in this element, other than the reputation of the electronic identification means itself, and the process of enrolment. | Not applicable |

| 28 | **Policy:** LoA's | **Reference:** 2.1. Enrolment – 2.1.2. Identity proofing and verification (natural person) |
|---|---|---|

*Low*

1. The person can be assumed to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity. 2. The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid.

3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.

*Substantial*

Level low, plus one of the alternatives listed in points 1 to 4 has to be met:

1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity and the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence; or

2. An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents; or

3. Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level substantial, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council(1) or by an equivalent body; or

4. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body.

*High*

Requirements of either point 1 or 2 have to be met:

1. Level substantial, plus one of the alternatives listed in points (a) to (c) has to be met:

(a) Where the person has been verified to be in possession of photo or biometric identification evidence recognised by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source; and the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source; or

(b) Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level high, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body and steps are taken to demonstrate that the results of the earlier procedures remain valid; or

(c) Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level high must be confirmed by a conformity assessment body referred to in Article 2(13)

| | | |
|---|---|---|
| of Regulation (EC) No 765/2008 or by an equivalent body and steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid. OR 2. Where the applicant does not present any recognised photo or biometric identification evidence, the very same procedures used at the national level in the Member State of the entity responsible for registration to obtain such recognised photo or biometric identification evidence are applied. | | |
| **Applicable to:** | **enrolment** | **authentication** |
| **Compliance:** | The process of enrolment of the ID-card (enrolling the biometric data) must be compliant to this element. As in the enrolment of the ID-card the biometric data are verified and the identity is verified against an authoritative source, the enrolment of the ID-card is supposed to be compliant to level High. If this would not be the case, the ID-card itself would not be sufficient for identity verification. The discussion could be about how the authoritative source should be invoked in the whole process, for example the birth certificate as breeder document. | Not applicable |
| **Trust factor Usability:** | The usability aspect is in the identity verification with photo or biometric identification evidence. The discussion could be how changes in looks should be assessed and if the match with the photo is sufficient. For example a person who has taken a photo with makeup and then for the application wears no makeup at all, is it the same person? Or persons with surgery. | Not applicable |
| **Trust factor Security:** | The security aspect is in the evidence and authoritative source. Literally for the evidence the risk of lost or stolen is mentioned. Additionally the discussion could be how the authoritative source should be invoked and if this is a secure process. For example is the data in the authoritative source correct and reliable. What happens if the authoritative source is not available. | Not applicable |
| **Trust factor Privacy:** | There seems no privacy aspect in this element. However the discussion could be how the authoritative source should be invoked and if this is a privacy enhancing process. For example does the authoritative source only portray necessary data for the enrolment process or maybe also has criminal or health references. | Not applicable |
| **Trust factor Reputation:** | There seems no reputation aspect in this element. However the discussion could be what the reputation of the authoritative source is. Maybe a lot of false negatives in the verification process, could have a bad reputation effect on the authoritative source itself and the enrolment process could have less trust because of it. | Not applicable |

| **29** | **Policy:** LoA's | **Reference:** 2.2. Electronic identification means management – 2.2.1. Electronic identification means characteristics and design |
|---|---|---|

*Low*
1. The electronic identification means utilises at least one authentication factor.
2. The electronic identification means is designed so that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs.
*Substantial*
1.The electronic identification means utilises at least two authentication factors from different categories.
2. The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.
*High*
Level substantial, plus:
1. The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential
2. The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | Not applicable | This element is about the authentication process.<br>The compliance of the ID-card seems no issue for level low. For level substantial, two factor authentication is necessary, but using the possession of the ID-card and the photo matching the live facial image, are two authentication factors from different categories and can only be performed by the person itself. So the proposed solution is supposed to be compliant to level substantial.<br>The additional stipulations for level high might seem harder to accomplish. The electronic identification means exists of a picture that is matched with a live facial image. After reading the picture from the chip, it is readily available for other use, and an electronic picture is always a "duplication". For compliance there must be additional safeguards so that a duplicated picture cannot be used. The solution for this is to be found in the Chip Authentication that is described in the ICAO standards. So the ID-card being compliant to the ICAO standards is supposed to be compliant to this element as well, if, and only if, for each authentication, the chip is to be verified with Chip Authentication. The mentioned high attack potential (which is from Common Criteria) is left for further research. The ID-card supposedly can be reliably protected against use by others because of the live facial image match. Eventually the proposed solution can be compliant to level High. |
| **Trust factor Usability:** | Not applicable | The usability aspect is in the whole authentication process: can a user do the whole process of NFC-reading the photo and match it with a live facial image. In certain situations (bruises in the face or other temporal disabilities) it could be a difficult. Protecting the ID-card against use by others and the high attack potential are also usability aspects, but in a negative way: can it be prevented that an attacker uses the means. Maybe technically it can be but the discussion could be that a user always can be forced by an attacker to do an authentication. It is unclear whether this scenario is to be investigated for a high attack potential. |
| **Trust factor Security:** | Not applicable | Several security aspects are mentioned explicitly, like duplication and tampering, as well as the protection against use by others (or attackers). However it is not stipulated *how* these security aspects are to be implemented, nor whether countermeasures are sufficient. The high attack potential is the mentioned goal, but it is not clear what level of security it really brings. So the discussion could be whether the attack potential as a methodology is sufficient. |

| | | |
|---|---|---|
| **Trust factor Privacy:** | Not applicable | There seem no privacy aspects in this element. However, it could be asked if the authentication process can be done in a privacy enhancing way, for example whether other people can look when the authentication process or be present “in the background”. The proposed solution is very likely to be used in a public space and maybe other could see that someone is performing the authentication process and just after that attack the user and grab its device. So maybe there should be awareness about how the process can be done by the user in a privacy enhancing way. |
| **Trust factor Reputation:** | Not applicable | There seems no reputation aspect in this element. However the discussion could be what the reputation of the high attack potential and/or Common Criteria is. For example the process of calculating / assessing the attack potential could be cumbersome and therefore not very effective. |

| **30** | **Policy:** LoA's | **Reference:** 2.2. Electronic identification means management – 2.2.2. Issuance, delivery and activation |
|---|---|---|

*Low*
After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed to reach only the intended person.
*Substantial*
After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed that it is delivered only into the possession of the person to whom it belongs.
*High*
The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | This element is about the delivery of the ID-card to the applicant / intended person and happens after the enrolment (issuance) itself. It is important to take place before the authentication process and therefore this element is analysed.<br>As for the ID-card the applicant "shall appear in person at least once" (ID-card: Article 10 Collection of biometric identifiers – Paragraph 1) it is supposed that the ID-card is compliant to level Low and Substantial. For level High an additional stipulation is made, about the activation process. Specifically this could be done via an activation code that is only to be known to the applicant and that is delivered in a secure way and/or it could be done with a first authentication to a special "activation service". With this activation process the ID-card is supposed to be compliant to level High.<br><br>What is not mentioned in this element, is how this activation service should work and thus that the authentication process can only be used if the means is activated. So probably an activation register has to be made, and this register is to be invoked before each authentication. Maybe a more efficient implementation can be done by having the activation status on the means itself. This is left for further research. | So probably an activation register has to be made, and this register is to be invoked before each authentication |
| **Trust factor Usability:** | The usability aspects are in the processes mentioned: delivery and activation. So the discussion can be whether the user can accomplish the delivery and the activation process. For delivery there are roughly two choices: pick-up and delivery via mail. A person could have a (temporal) disability which makes pick-up impossible but also delivery via mail could lead to problems, for example when a person has no validated mail address. So usability in delivery can really be an issue. Also the activation process can be less usable, and when it seems not possible, it could frustrate the process of authentication. Maybe therefore it is better to do the activation under supervision of the issuing authority, for example at the moment of pick-up or delivery (at the door). | Not applicable |
| **Trust factor Security:** | The security aspects are indirectly in the processes of delivery and activation. It is supposed to be a secure process which makes that the means is "delivered only into the possession of the person to whom it belongs". Both choices, of pick-up and delivery, supposedly can be secured in a sufficient way. Aspects that can be emphasized are the method of mail delivery (e.g. registered letter, special envelope) or the method of pick-up (in person with additional identity verification). | Not applicable |
| **Trust factor Privacy:** | There seem no privacy aspects in this element. However, it could be asked if the delivery and activation process can be done in a privacy enhancing way, for example whether other people can look when the delivery takes place and the activation is done. The proposed solution is very likely to be used in a public space and maybe other could see that someone is performing the activation process and just after that attack the user and grab its device. For mail delivery also privacy enhancing measures can be made, e.g. the envelope could be "anonymous", not indicating that it is a special shipment. Also pick-up could be done in a personal booth or | Not applicable |

| | | |
|---|---|---|
| | in public. So maybe there should be awareness about how the process can be done by the user in a privacy enhancing way and the issuing authority should also think about it. | |
| **Trust factor Reputation:** | There seems no reputation aspect in this element. However the discussion could be what the reputation of the delivery process is. For example the mail delivery could be very bad in a certain region and thus have a bad reputation. | Not applicable |

| **31** | **Policy:** LoA's | **Reference:** 2.2. Electronic identification means management – 2.2.3. Suspension, revocation and reactivation | |
|---|---|---|---|
| *Low / Substantial / High*<br>1. It is possible to suspend and/or revoke an electronic identification means in a timely and effective manner.<br>2. The existence of measures taken to prevent unauthorised suspension, revocation and/or reactivation.<br>3. Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met. | | | |
| **Applicable to:** | | **enrolment** | **authentication** |
| **Compliance:** | | All the assurance levels must be compliant to this element.<br><br>The electronic identification means in the proposed solution is the photo on the chip. So, according to this element, it should be possible to suspend / revoke the NFC-reading of the photo. However the main use of the photo is the (physical) identity verification which cannot and should not be suspended or revoked, unless when the ID-card is lost or stolen. Technically it might not be possible to suspend / revoke the NFC-reading of the photo and legally it should not be possible, so therefore the proposed solution could invoke a central register of lost or stolen ID-cards. It should also be possible to add the ID-card to the register "in a timely and effective manner". This register should then be invoked before each authentication.<br><br>Unauthorised suspension or revocation can be difficult to prevent in the case of the ID-card. If the ID-card is lost or stolen, anyone in possession of it could suspend or revoke it by destroying it (making it electronically unusable). So the compliance to 2 is questionable.<br><br>Reactivation (3) shall only take place under the same conditions as the enrolment. So it could be done by pick-up or delivery of a reactivation code and/or an authentication, or some similar process. | The register of lost or stolen ID-cards should be invoked before each authentication and therefor is an essential part of the authentication process to make it compliant. Also the earlier mentioned (re)activation register could be invoked at the same time. |
| **Trust factor Usability:** | | The usability aspects are in the processes mentioned: suspension / revocation / reactivation. So the discussion can be whether the user can accomplish the suspension and/or revocation. The problem might be that the user, at the moment that its ID-card is lost or stolen, has no idea that he should suspend or revoke the electronic identification means that the ID-card is used for. Awareness about this process could have a positive effect. Also "the timely and effective manner" is a usability aspect. It probably should be possible 24/7 although this is not made explicit in this element. | Not applicable |
| **Trust factor Security:** | | The security aspects are indirectly in the processes of suspension / revocation / reactivation. It is supposed to be a secure process which makes that the means, that is probably lost or stolen, is not being abused in the meantime or that its use is being monitored and investigated. It is likely that a person whose ID-card is lost or stolen might behave different and therefore be prone to (other) attacks. So maybe there should be awareness about how the process can be done by the user in a secure way and the issuing authority should also think about it. | Not applicable |
| **Trust factor Privacy:** | | There seem no privacy aspects in this element. However, it could be asked if the suspension / revocation / reactivation process can be done in a privacy enhancing way, for example whether other people can look when the suspension / revocation takes place. It is likely that a person whose ID-card is lost or stolen might behave different and therefore be | Not applicable |

| | | |
|---|---|---|
| | prone to (other) attacks. So maybe there should be awareness about how the process can be done by the user in a privacy enhancing way and the issuing authority should also think about it. | |
| **Trust factor Reputation:** | There seems no reputation aspect in this element. However the discussion could be what the reputation of the suspension / revocation / reactivation process is. For example going to the issuing authority for lost or stolen ID-cards might be cumbersome and thus have a bad reputation. | Not applicable |

| **32** | **Policy:** LoA's | **Reference:** 2.2. Electronic identification means management – 2.2.4. Renewal and replacement |
|---|---|---|

*Low*
Taking into account the risks of a change in the person identification data, renewal or replacement needs to meet the same assurance requirements as initial identity proofing and verification or is based on a valid electronic identification means of the same, or higher, assurance level.
*Substantial*
Same as level low.
*High*
Level low, plus: Where renewal or replacement is based on a valid electronic identification means, the identity data is verified with an authoritative source.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | Renewal or replacement of the electronic identification means (the photo) is not possible in the proposed solution (the ID-card) unless renewing or replacing the ID-card itself, having a new enrolment. Therefor compliance of the ID-card to this element is of no issue. | Not applicable |
| **Trust factor Usability:** | Renewal or replacement of an ID-card is a new enrolment, so not applicable | Not applicable |
| **Trust factor Security:** | Renewal or replacement of an ID-card is a new enrolment, so not applicable | Not applicable |
| **Trust factor Privacy:** | Renewal or replacement of an ID-card is a new enrolment, so not applicable | Not applicable |
| **Trust factor Reputation:** | Renewal or replacement of an ID-card is a new enrolment, so not applicable | Not applicable |

| **33** | **Policy:** LoA's | **Reference:** 2.3. Authentication – 2.3.1. Authentication mechanism |
|---|---|---|

*Low*
1.The release of person identification data is preceded by reliable verification of the electronic identification means and its validity.
2. Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline.
3. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.
*Substantial*
Level low, plus:
1.The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication.
2. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.
*High*
Level substantial, plus:
The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | Not applicable | For the validity check in general, the earlier mentioned lost or stolen register and the activation register could be used. For level substantial the check must be done through "dynamic authentication". The definition of "dynamic authentication" is in article 1, sub 3:<br>'dynamic authentication' means an electronic process using cryptography or other techniques to provide a means of creating on demand an electronic proof that the subject is in control or in possession of the identification data and which changes with each authentication between the subject and the system verifying the subject's identity;<br>Earlier:<br>"… the ID-card being compliant to the ICAO standards is supposed to be compliant to this element as well, if, and only if, for each authentication, the chip is to be verified with Chip Authentication. "<br>A Chip Authentication is a dynamic authentication on the possession factor.<br>The match of the photo with the live facial image is a dynamic authentication on the intrinsic factor.<br>So the proposed solution is supposed to be compliant with dynamic authentication.<br><br>The information to be "secured in order to protect against loss and against compromise, including analysis offline" can be applied to the photo that is NFC-read from the ID-card. It could be interpreted that the photo should not be stored anywhere, not even on the device itself. This however can make the matching process with the live facial image quite difficult. Therefore it is interpreted that the photo can be stored temporarily during the authentication process, whenever it is sufficiently secured.<br><br>The mentioned high attack potential (which is from Common Criteria) is left for further research. The ID-card supposedly can be reliably protected against use by others because of the live facial image match. |

| | | |
|---|---|---|
| | | Eventually the proposed solution can be compliant to level High. |
| **Trust factor Usability:** | Not applicable | The usability aspect is in the whole authentication process: can a user do the whole process of NFC-reading the photo and match it with a live facial image. In certain situations (bruises in the face or other temporal disabilities) it could be a difficult. Protecting the ID-card against use by others and the high attack potential are also usability aspects, but in a negative way: can it be prevented that an attacker uses the means. Maybe technically it can be but the discussion could be that a user always can be forced by an attacker to do an authentication. It is unclear whether this scenario is to be investigated for a high attack potential. |
| **Trust factor Security:** | Not applicable | Several security aspects are mentioned explicitly ("to protect against loss and against compromise, including analysis offline", "guessing, eavesdropping, replay or manipulation of communication by an attacker"). However it is not stipulated *how* these security aspects are to be implemented, nor whether countermeasures are sufficient. The high attack potential is the mentioned goal, but it is not clear what level of security it really brings. So the discussion could be whether the attack potential as a methodology is sufficient. |
| **Trust factor Privacy:** | Not applicable | There seem no privacy aspects in this element. However, it could be asked if the authentication process can be done in a privacy enhancing way, for example whether other people can look when the authentication process or be present "in the background". The proposed solution is very likely to be used in a public space and maybe other could see that someone is performing the authentication process and just after that attack the user and grab its device. So maybe there should be awareness about how the process can be done by the user in a privacy enhancing way. |
| **Trust factor Reputation:** | Not applicable | There seems no reputation aspect in this element. However the discussion could be what the reputation of the high attack potential and/or Common Criteria is. For example the process of calculating / assessing the attack potential could be cumbersome and therefore not very effective. |

| **34** | **Policy:** GDPR | **Reference:** Article 9 Processing of special categories of personal data – Paragraph 1 | |
|---|---|---|---|
| 1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. | | | |
| **Applicable to:** | | **enrolment** | **authentication** |
| **Compliance:** | | Biometric data (which is the photo) is explicitly mentioned and therefore "shall be prohibited". So processing the photo for enrolment cannot be compliant to this paragraph. An exception to this paragraph is to be sought in paragraph 2.<br><br>Looking at the preamble (51), there is an additional stipulation about the processing of photographs, which should not be considered of a special category, as they [the photographs] are covered by the definition of biometric data *only when* processed through a specific technical means allowing the unique identification or authentication of a natural person.<br>This is the case in the use for ID-cards, which confirms the conclusion that the processing of the photo is prohibited. | Biometric data (which is the photo) is explicitly mentioned and therefore "shall be prohibited". So processing the photo for authentication cannot be compliant to this paragraph. An exception to this paragraph is to be sought in paragraph 2.<br><br>Looking at the preamble (51), there is an additional stipulation about the processing of photographs, which should not be considered of a special category, as they [the photographs] are covered by the definition of biometric data *only when* processed through a specific technical means allowing the unique identification or authentication of a natural person.<br>This is the case in the use for ID-cards, which confirms the conclusion that the processing of the photo is prohibited. |
| **Trust factor Usability:** | | Since the solution is not compliant, this paragraph is not applicable. | Since the solution is not compliant, this paragraph is not applicable. |
| **Trust factor Security:** | | Since the solution is not compliant, this paragraph is not applicable. | Since the solution is not compliant, this paragraph is not applicable. |
| **Trust factor Privacy:** | | The whole article is about protecting the privacy of special categories of personal data. | The whole article is about protecting the privacy of special categories of personal data. |
| **Trust factor Reputation:** | | Since the solution is not compliant, this paragraph is not applicable. | Since the solution is not compliant, this paragraph is not applicable. |

| 35 | **Policy:** GDPR | **Reference:** Article 9 Processing of special categories of personal data – Paragraph 2 |
|---|---|---|

2. Paragraph 1 shall not apply if one of the following applies:
(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
(e) processing relates to personal data which are manifestly made public by the data subject;
(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

| **Applicable to:** | **enrolment** | **authentication** |
|---|---|---|
| **Compliance:** | In this paragraph an exception is to be sought for processing the photo for enrolment.<br>(a) explicit consent could be an exception;<br>(b) the purpose of having an ID-card is not in the field of employment / social security / social protection;<br>(c) there are no vital interests in the freedom of movement (which is the purpose of the ID-card);<br>(d) processing is carried out by the government, which is not a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim;<br>(e) the photograph is not manifestly made public by the data subject; | In this paragraph an exception is to be sought for processing the photo for enrolment.<br>(a) explicit consent could be an exception;<br>(b) the purpose of authentication for eGovernment is not in the field of employment / social security / social protection;<br>(c) there are no vital interests in the freedom of movement (which is the purpose of the ID-card);<br>(d) processing is carried out for eGovernment, which is not a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim;<br>(e) the photograph is not manifestly made public by the data subject; |

| | | |
|---|---|---|
| | (f) processing is not for the establishment, exercise or defence of legal claims;<br>(g) processing for the enrolment could be necessary for reasons of substantial public interest, on the basis of Union or Member State law, which is the freedom of movement;<br>(h) processing is not for medicine;<br>(i) processing is not public health;<br>(j) processing is not for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.<br><br>Only (a) and (g) seem to be applicable for compliance.<br>For the enrolment phase, it seems that "the substantial public interest" for processing of the biometric data is the freedom of movement, as portrayed in EU Regulation 2019/1157 on ID-cards. So compliance with (g) is not an issue. Therefore (a) is not analysed anymore. | (f) processing is not for the establishment, exercise or defence of legal claims;<br>(g) processing for the authentication could be necessary for reasons of substantial public interest, on the basis of Union or Member State law, which is the identification for eGovernment;<br>(h) processing is not for medicine;<br>(i) processing is not public health;<br>(j) processing is not for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.<br><br>Only (a) and (g) seem to be applicable for compliance.<br>For the authentication phase, the "substantial public interest" for processing of the biometric data is the identification for eGovernment. In EU Regulation 2019/1157 on ID-cards this processing is found in Article 11 – paragraph 6. However, that purpose is restricted so compliance with (g) seems to be an issue.<br>So the conclusion might be that if explicit consent is given before authentication, the photo can be used in the process. However an analysis should be made how this consent works during and after the process of authentication. |
| **Trust factor Usability:** | There is no usability aspect in this element, so not applicable. | There is no usability aspect in this element, so not applicable. |
| **Trust factor Security:** | There is no security aspect in this element, so not applicable. | There is no security aspect in this element, so not applicable. |
| **Trust factor Privacy:** | This element is about the purpose of personal data processing and its exceptions, like giving consent, which are privacy aspects. The whole article is about protecting the privacy of special categories of personal data. | This element is about the purpose of personal data processing and its exceptions, like giving consent, which are privacy aspects. The whole article is about protecting the privacy of special categories of personal data. |
| **Trust factor Reputation:** | There is no reputation aspect in this element, so not applicable. | There is no reputation aspect in this element, so not applicable. |

| **36** | **Policy:** GDPR | **Reference:** Article 9 Processing of special categories of personal data – Paragraph 4 | |
|---|---|---|---|
| 4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. | | | |
| **Applicable to:** | | **enrolment** | **authentication** |
| **Compliance:** | | This element is about the processing of biometric data, enabling Member States to further limit its use. However using the photo for the enrolment process is already in EU Regulation 2019/1157 on ID-cards, which is at Union level. So no limitations are to be expected at the Member State level. | This element is about the processing of biometric data, enabling Member States to further limit its use. Using the photo for the authentication process is somehow circumstantial in Article 11 – paragraph 6 of EU Regulation 2019/1157 on ID-cards. Further limiting of using the photo of the ID-card could be in Member State law and therefore the compliance should be investigated on a national level. So the proposed solution could be incompliant in certain Member States. (It is actually the case in the Netherlands!) |
| **Trust factor Usability:** | | There is no usability aspect in this element, so not applicable. | There is no usability aspect in this element, so not applicable. |
| **Trust factor Security:** | | There is no security aspect in this element, so not applicable. | There is no security aspect in this element, so not applicable. |
| **Trust factor Privacy:** | | The whole article is about protecting the privacy of special categories of personal data. | The whole article is about protecting the privacy of special categories of personal data. |
| **Trust factor Reputation:** | | There is no reputation aspect in this element, so not applicable. | There is no reputation aspect in this element, so not applicable. |