Dutch Identity Matching:

The Devil's in the Details

Master thesis submitted to Delft University of Technology

in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in **Complex Systems Engineering and Management**

Faculty of Technology, Policy and Management

by

Anton Welling de Arruda

Student number: 5352886

To be defended in public on November 16th, 2022

Graduation committee

Chairperson	:	Dr.ir. G.A de Reuver, Engineering Systems and Services
First Supervisor	:	Prof.dr.ir. N. Bharosa, Engineering Systems and Services
Second Supervisor	:	Mr. J.M. Kooijman, Multi-Actor Systems
External Supervisor	:	MSc. T. Speelman, Ministry of the Interior and Kingdom Relations

Management Summary

The revision of the eIDAS Regulation proposes the implementation of a European digital identity wallet for citizens to authenticate themselves across the EU. The process to decide if a person already has an account at the service where they seek to authenticate themselves is called identity matching. Regulated and public Dutch Relying Parties and the Dutch government are not always able to assess whether a citizen authenticating themselves has a pre-existing record at the Relying Party or in the Dutch national registry. Moreover, the current dependency on the Dutch central identity matching service creates a Single Point of Failure. Besides these reliability problems, privacy issues such as profiling data minimization must be accounted for. To this end, this research proposes three possible solution directions for solving these problems: a government-centric, wallet provider-centric, and a hybrid solution direction. The design of the solution directions follows a design science research methodology. The possible solution directions are evaluated by experts in focus groups to elicit the benefits and the barriers which these experts identify as relevant factors for accepting a solution direction. These factors are categorized using the TOE model, which is adapted to suit the current context. Expert evaluations during the focus groups have resulted in factors which relate to the organizational, technological, and external environment of the solution directions. The evaluation uncovered tradeoffs which the Dutch Ministry of the Interior must make to choose between one of the proposed solution directions: reuse of infrastructure at the cost of citizen privacy, or more privacy for citizens at the cost of additional logic requirements needed for the identity wallet. Based on the privacy and reliability requirements and the objective of the Dutch government to give citizens more control over their personal data, the wallet provider-centric solution direction is the most fitting choice of the three proposed solution directions. The explication of the problem, requirements, and solution directions can be used as a starting point in the exploration of new solution directions for the identity matching problems. More research is needed on other possible solution directions than are proposed in this research and their viability to meet the objectives of the Dutch government and deadlines set by the European Commission.

Acknowledgements

Through this short message, I would like to thank the people that made it possible for me to complete the work that lies in front of you. My supervisors from the TU Delft, Nitesh, Mark, and Joyce, for their proactive and positive attitude towards the project. This gave me the feeling that we wrote this thesis as a team.

I am deeply grateful for the competent team and supervision which I enjoyed during my thesis internship at the Dutch Ministry of the Interior. In particular to Tim Speelman and Alexander Bielowski, who spent countless hours reviewing my work. Your knowledge and insights have made this thesis to what it is today.

Content

Chapter 1: Introduction and Problem Statement

1.1 Introduction

"*We must make this Europe's digital decade*"
- von der Leyen (2020), State of the Union Address

To this end, von der Leyen promised the European Commission (hereafter: Commission) would propose a secure European digital identity, available to all citizens of the European Union (EU) (hereafter referred to as 'citizens'). The development of a European digital identity is not new. Most notably for this research is the 2014 eIDAS 1.0*[1] regulation (Regulation 910/2014). This regulation has set standards for digital identification methods across the European Union (EU) for citizens and legal persons. The goal of this regulation is to strengthen the European Single Market by promoting confidence and convenience in cross-border electronic transactions. These benefits have not come to fruition as initially planned: since the regulation came into effect in September 2018, only 59% of the EU population (living in 14 Member States) can use an electronic national identity document cross border. To achieve the eIDAS' goals, the Commission has proposed an amendment of the regulation (eIDAS 2.0)* which mandates a 'European Digital Identity Wallet' (EUDI-Wallet)*. This is a nationally provided mobile application with which each EU citizen can identify themselves at every public institution in the EU, as well as at private parties which rely on unique identification for the provision of their services (European Commission art. 12b, 2021).

In some use cases, the party where a citizen authenticates themselves (i.e. Relying Party (RP)*) must be able to uniquely distinguish this citizen from others. For instance, a social security office must know who is applying for their services, and if they have applied in the past. The process to decide if a person already has an account at the service where they seek to authenticate themselves is called identity matching (WG3, 2022). As of now, the EU has not adopted a standard way the identity matching process should be carried out. The proposed amendment and the implementation guide have however set some guidelines on what data is used to match two identities: with Person Identification Data (PID) (European Commission art. 3(55), 2021). Under eIDAS 1.0, the PID consists of a person's current family name(s), current

[1] Terms marked with an * are defined in Appendix X

first name(s), date of birth, and a unique identifier which is as persistent as possible (Regulation 2015/1501). To ensure a coordinated approach and to avoid fragmentation of the implementation of the wallet, Member states are asked by the Commission to draft a so called ‘Toolbox’. The Toolbox should include a technical architecture and reference framework, a set of common standards and technical references covering at least all aspects of the functionalities and interoperability of the identity wallet (European Commission, 2021). The Dutch Ministry of the Interior and Kingdom Relations (hereafter: Dutch Ministry of the Interior) is tasked with implementing the eIDAS regulation and its revision in the Netherlands (Nora, 2017).

1.2 Problem statement

Dutch RPs are not always able to assess whether a citizen authenticating themselves with a foreign eID mean* has a pre-existing record at that RP. Moreover, the current process relies on a Single Point of Failure (SPOF) since each identification request depends on two functionalities of the Dutch government. This dependence on the Dutch government for unique identification brings forth privacy concerns such as the Dutch government having access to each identification request of a citizen.

The Dutch Ministry of the Interior lacks an overview of different solution directions for the privacy and reliability problems of uniquely identifying citizens, and what implications these solution directions have on their requirements. Reviewed literature does not fulfill this demand because it does not offer a complete description of the problems and a set of possible solution directions and their implications on the privacy of citizens and the reliability of finding a correct match. Moreover, not incorporating stakeholder requirements is one of the common reasons for the failure of IT projects of the Dutch government (Tweede Kamer, 2014).

The Dutch government, and thereby the Ministry of the Interior, has the objective of providing citizens a digital identity and more control over their personal data (van Huffelen, 2022; VVD et al., 2022). This research therefore seeks to design possible solution directions which the Dutch Ministry of the Interior can take which meet their requirements relating to privacy and reliability. The Dutch Ministry of the Interior is chosen as the problem owner for this research. To this end, the research seeks to answer to following research question:

Which solution directions can be taken to meet the requirements of the Dutch Ministry of the Interior for solving the privacy and reliability problems related to uniquely identifying a citizen using a foreign EUDI-Wallet to identify themselves at a Dutch regulated or public RP?

The research is scoped to unique identification at Public and regulated RPs because these are often required by law or for the provision of their services to uniquely identify an individual. Therefore, these parties are obliged to accept the use of the EUDI-Wallet according to eIDAS 2.0 (European Commission art. 12b, 2021). For this research, RPs in the transport, utilities, banking and financial services, healthcare, education, and telecommunication sectors are considered to be regulated RPs. Since the Dutch notified eID mean (DigiD) is already linked with the BSN* (Dutch citizen service number), its users are already uniquely identified when they onboard their DigiD (Moniava et al., 2008). Under eIDAS 2.0, citizens from other MSs might not be able to have their BSN linked to the PID in their EUDI-Wallet at onboarding due to their EUDI-Wallet being supplied with PID from another MS, which may not have access to the BSN. To scope the research, unique identification of a citizen using a Dutch eID mean or EUDI-Wallet is left out of the scope of this research.

Chapter 2: Research Design

2.1 Introduction

This chapter provides an overview of the research methodologies and the research methods used per sub-question.

2.2 Sub-questions

The following sub-questions have been chosen to structure the answer to the main research question, as well as ensuring the completeness of the answer:

Which solution directions can be taken to meet the requirements of the Dutch Ministry of the Interior for solving the privacy and reliability problems related to uniquely identifying a citizen using a foreign EUDI-Wallet to identify themselves at a Dutch regulated or public RP?

To answer this question, first a description is given of how a citizen using a foreign eID mean is currently uniquely identified in the Netherlands. This is followed by an identification of the privacy and reliability problems which are associated with the current process of unique identification. This is followed by a description of the solution directions which are discussed for these problems in literature on identity matching and identity management. After the privacy and reliability problems and known solution directions are described, the requirements of the Dutch Ministry of the Interior to solve these problems are elicited. This is followed by possible solution directions which the Ministry can take to solve the privacy and reliability problems. The solution directions are then compared to the requirements and evaluated to elicit the benefits and barriers they identify for each solution direction. To structure the answer to the research question, the answer is composed by the sum of the following sub-questions:

SQ1: *Which privacy and reliability problems arise in the process of uniquely identifying a citizen using a foreign EUDI-Wallet to identify themselves at a Dutch regulated or public RP?*

SQ2: *Which solution directions can be taken to solve the identified problems and meet the requirements of the Dutch Ministry of the Interior for uniquely identifying a citizen using a foreign EUDI-Wallet to identify themselves at a Dutch regulated or public RP?*

SQ3: *Which benefits and barriers do experts expect for the acceptance of a solution direction?*

2.3 Methodologies

2.3.1 Solution Direction Designs

The second sub-question proposes new solution directions for the process of uniquely identifying a foreign EUDI-Wallet at a Dutch regulated or public RP. Design science is used to structure and guide the design of new processes for uniquely identifying a foreign EUDI-Wallet. It is defined by Johannesson & Perjons (2014) as: *"the scientific study and creation of artefacts as they are developed and used by people with the goal of solving practical problems of general interest."*. The following five design science methodologies are reviewed in this section to assess their fit with the research question:

1. Hevner et al. (2004)
2. Peffers et al. (2007)
3. Sein et al. (2011)
4. Johannesson & Perjons (2014)
5. Vom Brocke & Maedche (2019)

According to Hevner et al. (2004), design science seeks to:

1. develop and verify theories; and
2. extend the boundaries of human and organizational capabilities by creating innovative theories.

To this end, Hevner poses three cycles (relevance, design, and rigor) which continuously iterate between each other. A guideline of the rigor cycle is the addition and communication of new knowledge to the domain of design science research (Hevner, 2007). Vom Brocke & Maedche (2019) and Johannesson & Perjons (2014) attest to this guideline, by stating that "the goal of design science research is to generate prescriptive knowledge about the design of information systems". Vom Brocke & Maedche (2019) observe that early design science research focused on the design of artefacts, such as the research of Peffers et al. (2007).

This thesis seeks to combine both perspectives on design science research: contribute to the knowledge on designing artefacts and, if feasible, design an artifact. The design phases of Peffers et al. (2007) and Johannesson & Perjons (2014) are similar. The methodology of Johannesson & Perjons however offers an elaborate description of the steps to be taken in the research, while the paper of Peffers et al. (2007) contains little to no explanation on these activities. Therefore, the methodology of Johannesson & Perjons (2014) can prove useful guidance during the design process.

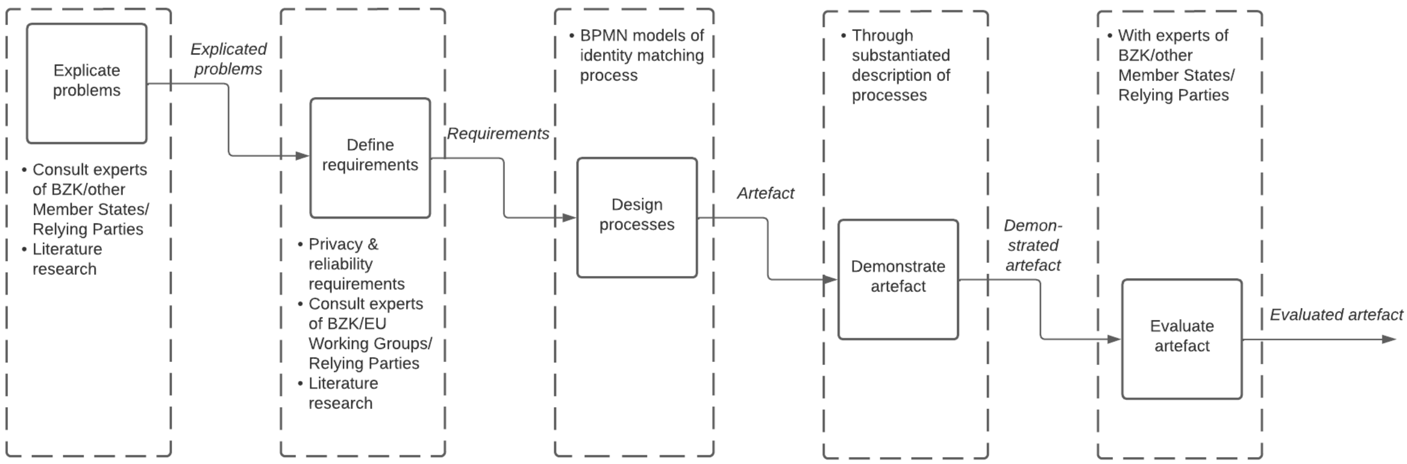

Figure 1: Design Science Research Flow

First, the reliability and privacy problems which relate to uniquely identifying a citizen with a foreign eID mean are explicated. This is done through desk research in the form of a literature review and interviews with experts on the subject. Three interviews are held to explicate the problem. The participants are employees or contractors of the Dutch Ministry of the Interior, the Dutch National Office for Identity Data (RvIG), the Dutch tax office, and A-SIT (an organization which develops cross-border eID solutions for the Austrian government). What these interviews contribute to knowledge regarding the problem and the roles they fulfill at their organizations is summarized in Appendix C. A possible limitation is the possibility that the problem is not exhaustively explicated due to the dependance on the consequences of future circumstances. This is due to the eIDAS 2.0 not having gone into effect at time of writing. It is possible that unexpected problems will manifest.

Second, reliability and privacy requirements are also elicited through a literature review and the same three interviews. The reason for this method is that the requirements for a solution direction are partly noted in literature, legislation, and official governmental publications. Experts are interviewed to uncover requirements which are possibly not available in these publicly available documents. A limitation of the set of the requirements is the considerable chance of them becoming outdated due to regulatory uncertainty.

Third, desk research and interviews are held to design the solution directions. The different options for identity matching solution directions can be found in literature and practice. Therefore, besides desk research, two interviews are held: one with someone who is responsible for setting up the identity matching process for eID means in the Netherlands, and one with the person responsible for the development of the polymorphic encryption scheme used to create identifiers for eID means in the Netherlands. Feasibility issues lie in not considering all possible designs, not finding a design which solves the problems, and the designs not being detailed enough for a thorough evaluation.

Fourth, the solution directions are demonstrated by a substantiated description of how the processes flow and why the process would work in practice (e.g. through certain cryptographic assurances). Since the solution directions are not tested in a real environment, the designs have the risk of returning false positives (i.e. being judged better demonstrated better than they in fact are).

Fifth, the solution directions will be evaluated through interactive focus groups. How and what will be evaluated is described in detail in the following section.

2.3.2 Evaluation of Solution Directions

The evaluation is carried out to answer the third sub-question: *Which benefits and barriers do experts expect for the acceptance of a solution direction?*

This will be answered by eliciting the expected benefits and barriers which experts of EU governments and Dutch regulated RPs foresee. Since the solutions have not been implemented at time of writing, the benefits and barriers in practice can differ from how experts expect them to be. Therefore, they are defined as *expected* benefits and barriers. The evaluation will be summative, meaning that the elicited benefits and barriers are not addressed in the design in a later iteration. Since the processes have not been implemented, the evaluation risks resulting in false positives due to the design being judged better than it would be in practice (Johannesson & Perjons, 2014). This limitation is considered when interpreting the results. The variables which influence the willingness of these experts to accept will result from their evaluation.

As with design science research methodologies, there are multiple theoretical models which show the relation between factors which influence the acceptance of technology. According to Oliveira & Martins (2011) and Dube et al. (2020), the most common models for IS and IT acceptance are the Technology Acceptance Model (TAM) (Davis, 1986), Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003), DOI (Rogers, 1995), and the TOE framework (Tornatzky et al., 1990). Since the DOI and TOE framework are the only two of these models which have been widely applied to technology acceptance on an organizational level instead of an individual level, these two will be reviewed for their applicability in this research.

According to the DOI theory, innovativeness is related to independent variables such as individual characteristics, internal organizational structural characteristics, and external characteristics of the organization. The TOE framework (figure 2) distinguishes three aspects of a technology's context which influence the willingness to accept a technology: technological context, organizational context, and environmental context. The TOE are similar and consistent to DOI (Oliveira & Martins. 2011). However, the TOE contains an additional component which can foster or constrain technology acceptance: the environmental component, which is of importance to the current context (e.g. regulatory requirements, infrastructure from wallet providers). Moreover, while DOI has been applied widely to an organizational level, researchers have challenged the validity of its application to complex technological innovation acceptance on an organizational level (Attewell, 1992; Wang & Lo, 2016). Therefore, the TOE model is used as a basis for analyzing the variables for the acceptance of an identity matching solution (figure 2).

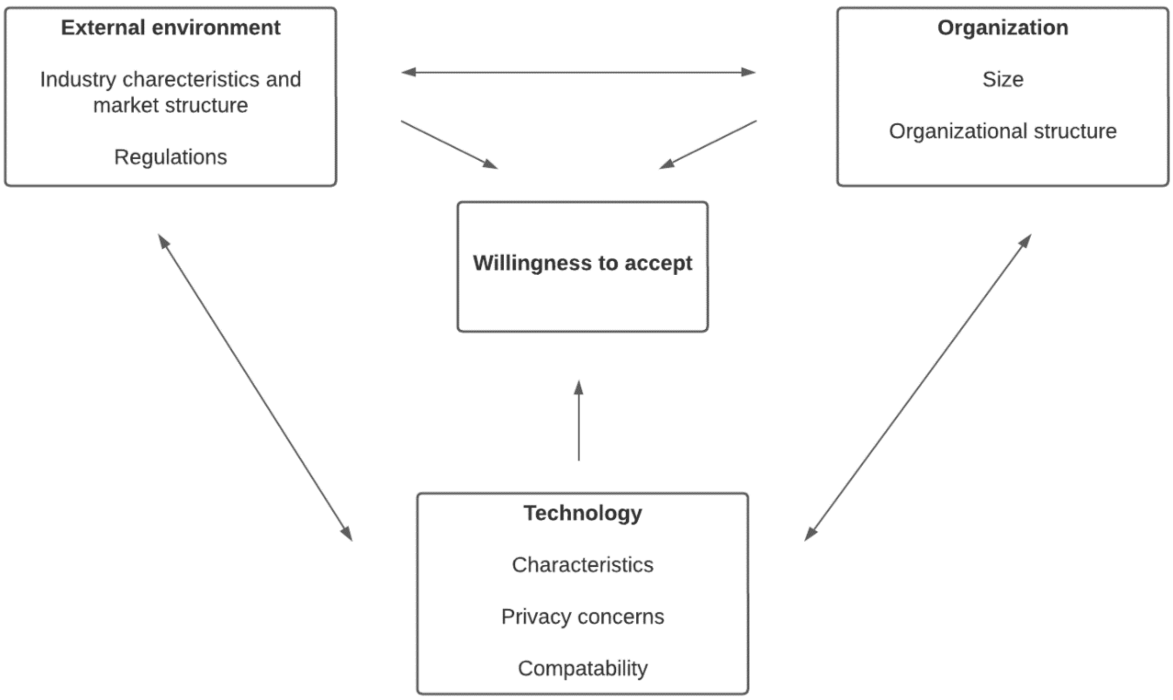

Figure 2: Original TOE Framework (Tornatzky et al., 1990)

Any borrowed theory should match the context of application. Since the TOE model is largely applied in the private domain, some suggested variables (e.g. competitive advantage) from previous research are not directly applicable to the current context. Also, no research has been found regarding the acceptance of identity matching processes nor of identity management models in the Dutch eID context. Therefore, there is no set of validated variables and their relationships to assess their influence on the acceptance of a certain solution direction. This research seeks to find these variables and their influence (i.e. being a benefit or barrier) on the acceptance of a certain solution direction. This mirrors the approach of Bradford et al. (2014), which also seek to find previously unknown variables which can be categorized according to the TOE model. The adapted TOE model is visualized in figure 3.

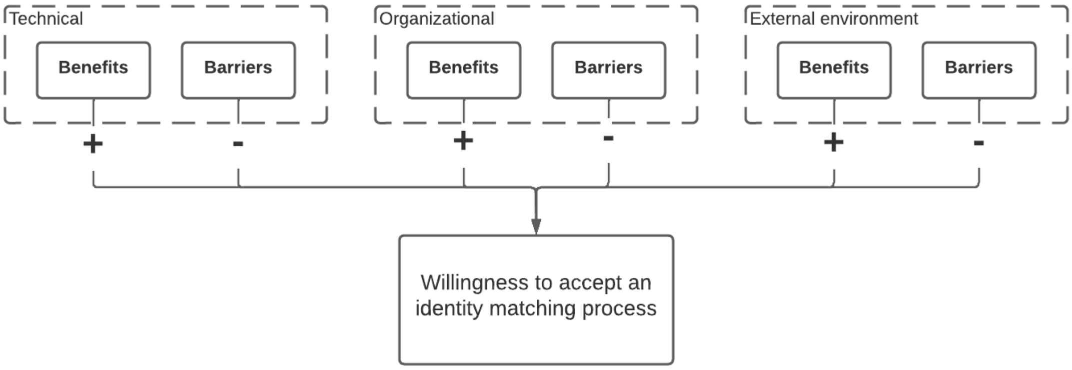

Figure 3: Adapted TOE model (inspired by Bradford et al. (2014))

The TOE model has its limitations. It has been described as a generic theory (Baker, 2012). Moreover, it is solely a classification of categories, and some argue that additional theory is needed to explain specific variables and their relations (Dube et al., 2020). The genericness and the fact that not all variables are set in advance however can be advantageous for this research due to its novelty: the benefits and barriers of a solution direction can depend on unknown (future) circumstances such as regulatory changes and the discovery of new privacy risks.

2.3.3 Focus Groups

The processes are evaluated through two focus groups, since this is a suitable method for understanding and interpreting the perspective of participants (Johannesson & Perjons, 2014). Moreover, multiple experts can participate in one session, which is beneficial considering the time constraints of this research. Lastly, meeting in groups with different backgrounds can increase imaginative and creative output of experts (Johannesson & Perjons, 2014).

The content of the two focus groups were the same. The first focus group did not allow time to plenarily discuss all input from participants. Therefore, a second focus group was organized to allow enough time to discuss all input from participants. The goal of the focus groups is to explain the process designs to the participants, after which they can give their opinion on the designs. The focus groups started with a presentation on the scope of the research and the process designs. Participants could ask questions regarding the designs, the problem, and the scope. The input was only gathered after all participants indicated that they understood the functionalities of the different solution directions.

A threat of focus groups is that some participants can influence other participants by leading the discussion in a certain way which impedes the input of participants with different opinions (Johannesson & Perjons, 2014). To account for the threat of participants monopolizing discussions, before a plenary discussion was held, participants had time to write their input on a Miro-board. Another drawback of focus groups is observer dependency: results are dependent on the interpretation and analysis of the researcher (Johannesson & Perjons, 2014). To give insight into how the input of participants is analyzed, Appendix G shows the written and verbal input of participants, and how this input is abstracted.

There were three categories of feedback which the participants could give for each solution direction: benefits, barriers, and points to consider. After the participants had given their input, they were invited to explain their input verbally to start a discussion amongst the participants and to clear up possible ambiguities in their written input. A secretary kept notes of input which was given verbally which was not present on the Miro-board, since moderation of a focus group is a full-time job (Johannesson & Perjons, 2014). The focus groups are held online to accommodate experts from other MSs.

Each benefit, barrier, and point for further consideration is abstracted to create a comprehensible overview of the factors which influence experts to accept a solution direction. The abstraction also helps in comparing the solution directions and finding tradeoffs. For example, a benefit named of the hybrid solution direction "Should eliminate tracking of citizens" is abstracted to the factor "Tracking of citizens". This is also done for the barrier of the central approach "Tracking can get an issue", which makes it clear that both the benefit and the barrier relate to the same evaluation criterium "Tracking of citizens".

In total, 14 experts participated in the focus groups. Thirteen experts participated in the first focus group, and seven participants he second focus group. In the second focus group, there was one participant who had not been present during the first focus group. The participants were either employed at the Dutch Ministry of the Interior, the European Commission, the Dutch tax office, public bodies from MSs, or hired as external experts for one of these organizations.

Chapter 4: Literature Review

4.1 Introduction

This chapter composes an answer to the first sub-question:

SQ1: *Which privacy and reliability problems arise in the process of uniquely identifying a citizen using a foreign EUDI-Wallet to identify themselves at a Dutch regulated or public RP?*

This will be done by firstly describing how a foreign eID is currently uniquely identified by the Dutch government and Dutch regulated or public RPs. Thereafter, privacy problems which arise in this process of unique identification are identified. Literature on identity management models is reviewed to assess whether the identified problems have also been identified in literature and whether literature proposes an answer to the privacy problems. Lastly, reliability problems of unique identification are explained, together with suggestions from experts and literature on how to solve the reliability issues.

4.2 Literature Review Approach

The 'Preferred Reporting Items for Systematic Reviews and Meta-Analyses' (PRISMA) approach of Moher et al. (2009) is used to structure the literature review.

The search bank Scopus is used as the basis of the literature search. From the articles found in this database, additional articles are found through snowballing. Table 10 Appendix B shows the search terms used on Scopus together with the amount of hits it returned, and the number of duplicates with the search query above it. Table 11 indicates which articles have been found through searches on Google and Google Scholar. Google has been used because none of the articles found on Scopus describe how a foreign eID mean is uniquely identified in the Netherlands.

Besides Scopus and Google, the literature review is complemented by interviews to complement the knowledge from literature, since the problem is not fully explicated in academia. The relevant passages from these interviews are summarized in Appendix C.

The following criteria have been applied to narrow down the number of articles included in the review of identity *matching* literature:

- *Field:* Identity matching between Member States.
- *Topic*: Included articles need to discuss the process of identity matching between MSs, the problems related to this, or solutions for the problems. Due to the limited number of articles on identity matching in the context of eIDAS, articles from the similar Single Digital Gateway (SDG) Regulation are also included (Regulation 2018/1724).
- *Study design*: Both empirical and qualitative studies have been consulted. Since the problems are discussed in a qualitative manner (how do the problems occur), and empirical studies offer insight in the scope of the problem (how many times do the problems occur).
- *Language*: Only articles in Dutch and English are eligible.
- *Year of publication*: Only articles which are published after the eIDAS 1.0 regulation (august 2014) are included.
- *Publication types*: Peer-reviewed articles, reports of research institutes, European working group documents, and expert interviews were eligible for review. The reason for the broad scope of documents used is due to the limited description of the identity matching processes and problems in the Netherlands. To get a broad view of the current state, multiple types of sources are used.

The following criteria have been applied to narrow down the number of articles included in the review of identity *management* literature:

- *Field:* Identity management models.
- *Topic*: Studies need to include terminologies, theories, models, or architectures of identity management, so these can be compared to the current eIDAS identity matching process.
- *Study design*: Only qualitative studies have been consulted which give describe identity management models.
- *Language*: Only articles in Dutch and English are eligible.
- *Year of publication*: Only articles which are published after the year 2004 are included, since this the first year in which more than one article appears on identity management in the context of the provision of online services in the Scopus database.
- *Publication types*: Only peer-reviewed articles and books were eligible for review. There are much content on identity management, only these published sources were considered for quality considerations.

4.3 How it works

4.3.1 Example of Unique Identification.

To explain how citizens are uniquely identified in the current eIDAS network in the Netherlands, firstly, an example of a physical identification request is shown in figure 4 and 5. This will aid the understanding of why the eIDAS regulation has been put into effect, as well as help in the understanding of the solution directions which will be discussed later. The actors and their roles in this identification process are listed in table 1.

Table 1: Actors and their roles

Actors	Roles
Citizen	Seeks to access public and/or private services
Identity Provider (IdP)*	Issues and attests identity attributes to citizens
Relying Party (RP)	The party where the citizen seeks access to a service

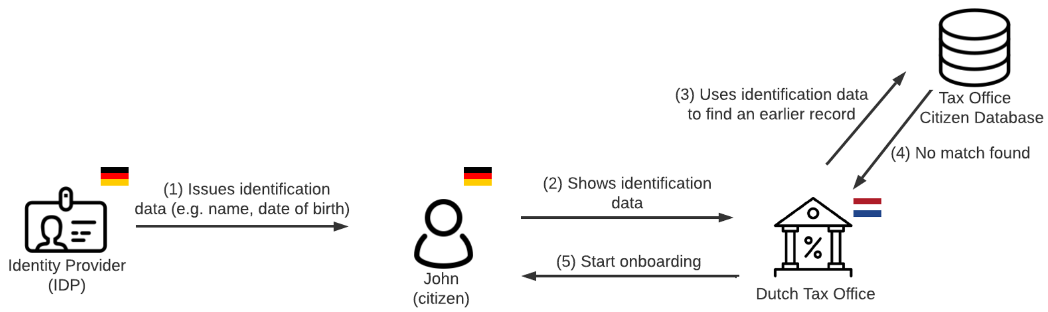

Figure 4: Onboarding

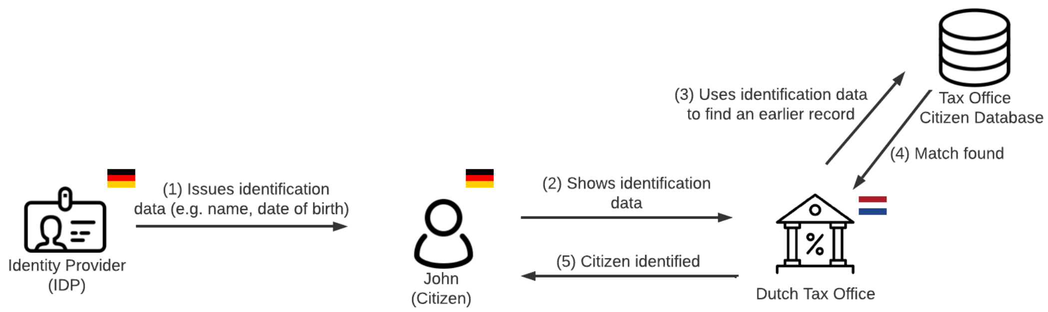

Figure 5: First and subsequent matches

Figure 4 illustrates an example of a German citizen (John) who seeks to authenticate himself at the Dutch tax office. An identity provider, in this case the German government, issues identification data to John (e.g. his name and date of birth) and attests these attributes in official documents (e.g. passport and birth certificate). Due to the authenticity features of the official documents, the tax office can trust that the identity attributes on these documents pertain to John. In figure 4, John has never authenticated himself before at the tax office, and therefore there is no record at the tax office which matches his identification data. Because of this, the tax office starts the onboarding process. In figure 5, John is already listed in the tax office's database, and is therefore matched to his existing record.

4.3.2 The Dutch eIDAS 1.0 Identity Matching Architecture.

Contrarily to the example above, most of the interactions between citizens and the Dutch government occurs through digital channels (52.7% in 2016) (Kanne & Löb, 2016). To ensure that citizens can securely access services provided by public RPs across the EU, eIDAS 1.0 sets standards on the digital identification process. Figure 7 depicts a simplified version of how currently an identification request is handled in the eIDAS network of a citizen using a non-Dutch eID mean* at a Dutch RP.

The actors, their functions, and the roles these functions fulfill in the current Dutch electronic identification process of eIDAS 1.0 are listed in table 2 and visualized in figure 7. The description of their roles is scoped to what is relevant for ensuring unique identification of citizens at Dutch RPs. The actors may also fulfill other roles. The Dutch eIDAS Connector for instance also handles identification requests of Dutch eID means seeking identification in other MSs. This is out of the scope of this research, and therefore not included in the role description.

Table 2: Functions and their roles (based on Nora, 2017)

Actor	Function	Roles
eID Mean Provider	eID Mean	Authenticate the citizen.
Foreign Member State	eIDAS Node* of Home Member State	Sends PID of citizen to the Dutch eIDAS Node.
Dutch Ministry of the Interior	Dutch eIDAS Connector	Tasked with connecting the foreign eIDAS Nodes to the eID Broker. It contains a mapping table of all incoming identification requests which contain: the eID Means used per citizen and the pseudonyms which are used to identify at a RP.
	eID Broker	Handles identification requests of citizens for Dutch RPs. Functions as a sort of proxy to relieve RPs of the burden of handling identification requests. Checks which identifier the RP is authorized to receive.
	BRP Connector	Tasked with assessing whether a citizen authenticating themselves with a foreign eID mean is present in the national registry of natural persons (BRP)*.
	BSN Connector	Tasked with the encryption and decryption of identifiers which citizens use to identify themselves at a RP.
Relying Party (RP)	Relying Party (RP)	The party where the citizen seeks to access public and/or private services. The RP relies on the unique identification of the Dutch eIDAS Node to uniquely identify a citizen.
Citizen		Can supply additional identification data when asked.

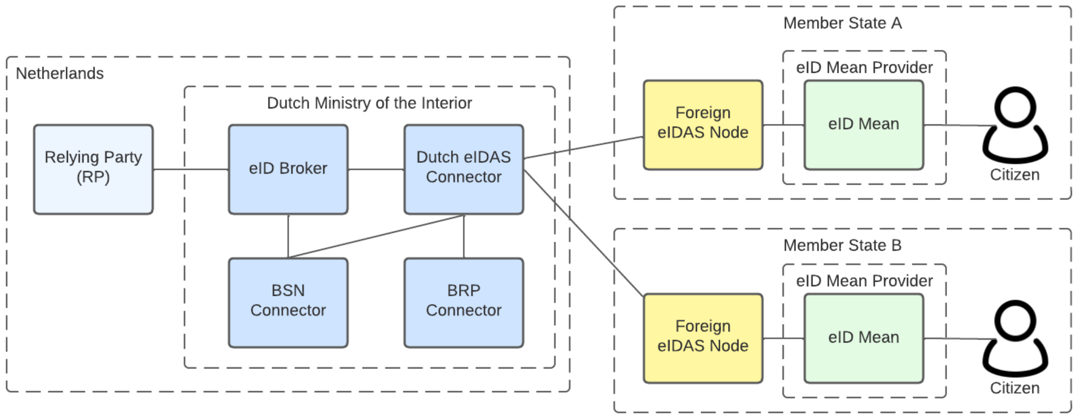

Figure 7: Visualization of the Dutch eIDAS 1.0 architecture

In the Netherlands, online unique identification in the public sector is often established by comparing a citizen's Citizen Service Number (CSN) to a record of that citizen at a public RP (Moniava et al., 2008). The possession of a CSN is for instance required for accessing tax records. There are however public services which do not require unique identification with an CSN: for example when requesting the photo taken of the car responsible for a speeding ticket at the CJIB (the Dutch Central Judicial Collection Agency). The citizen who is responsible for the speeding violation has already been uniquely identified through the license plate, whereafter this citizen receives a letter with a code to enter on the site of the CJIB. Since the person who request this photo has received a letter with a code to enter on the site of the CJIB, thereby proving the validity of the request, it is therefore not seen as necessary uniquely identify the citizen again on the site of the CJIB with the citizens CSN.

Besides the CSN, the following four unique and persistent identifiers are used in the Dutch eIDAS identity matching process of foreign eID means (Nora, 2017; Verheul, 2019). The way in which they are used is described in the next section.

- **eIDAS identifier**: the identifier which is used in the eIDAS minimum data set (PID). For each MS, the identifier is formatted as: [home_MS/destination_MS/ID (e.g. GE/NL/1234AB)
- **PP-EU**: a polymorphic pseudonym* which is derived from the eIDAS identifier. This identifier is used for Dutch RPs in the private sector.

- **PP-BSN**: a polymorphic pseudonym which is derived from the BSN. Every eID mean a citizen uses receives a different PP-BSN. The BSN is only derivable from the PP-BSN by Dutch RPs which have a decryption key. This key is only given to authorized RPs.
- **PP-RP**: a pseudonym specifically for each Dutch RPs. It is a pseudonym of the former two identifiers (the PP-EU, PP-BSN), constructed by encrypting this identifier with the public key of the RP. Therefore, only the authorized Dutch RP can derive the decrypted identifier. A RP does not have access to the PP-EU, PP-BSN, and PP-PS: they are only for internal communication between the Dutch eIDAS Connector and the BSN Connector.

4.3.3 The Dutch eIDAS 1.0 Identity Matching Process.

A Simplified BPMN diagram of the process is illustrated in figure 8. The whole process can be consulted at: https://antonwelling.nl/identity-matching-current-state/

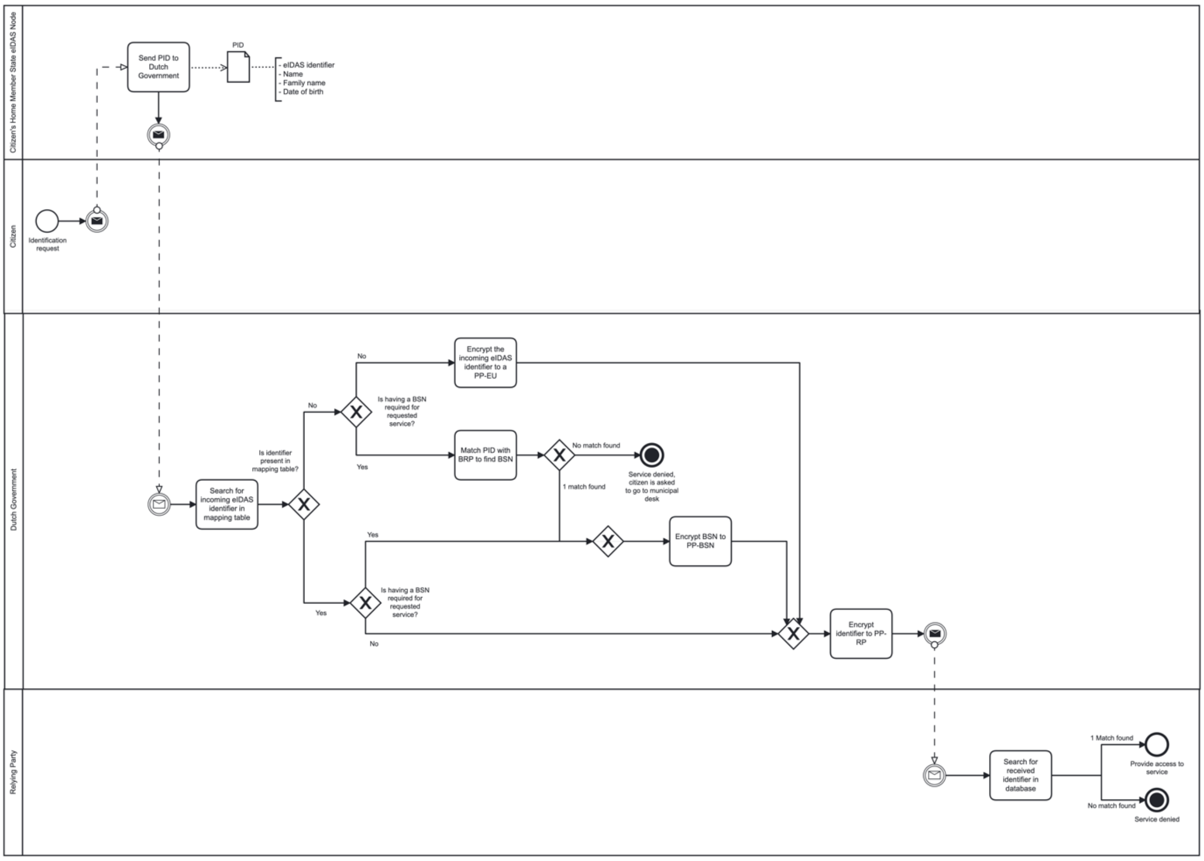

Figure 8: Simplified BPMN

The process starts with a citizen seeking to access a service at a Dutch RP using a foreign eID mean. The RP sends the request through to the eID Broker, which sends the request to the Dutch eIDAS Connector. The Dutch eIDAS connector checks if a BSN is necessary for the service requested by the citizen. Thereafter, the eIDAS Connector requests the citizen's PID from the foreign eIDAS node.

When the foreign eIDAS node of the MS where the eID is notified has shared the PID (names, date of birth, and unique identifier), the Dutch eIDAS Connector searches their mapping table for the provided eIDAS identifier. The mapping table contains records of previous identification attempts. It records citizen's eIDAS identifiers together with an encrypted version of their BSN (PP-BSN) and RP specific identifiers (PP-RP). The search for the eIDAS identifier in the mapping table returns either one of two results: the eIDAS identifier is found in the mapping table, or it is not. If the eIDAS identifier is not found, one of the following two tasks are executed (visualized in figure 9):

1. **Identifier not found** in mapping table & **BSN is required**: It is assumed to be the citizen's first identification attempt because the eIDAS identifier is not present in the mapping table. Since the requested service requires a BSN, the citizen is asked to send their BSN.

2. **Identifier not found** in mapping table & **BSN is not required**: The BSN Connector is requested to encrypt the incoming eIDAS identifier. The Netherlands can assume that the eIDAS identifier is unique (i.e. only corresponding to one citizen). Since this identifier can change over time, or a citizen can sometimes have multiple identifiers, besides the encrypted identifier, also the citizen's full name and date of birth are shared with the RP.

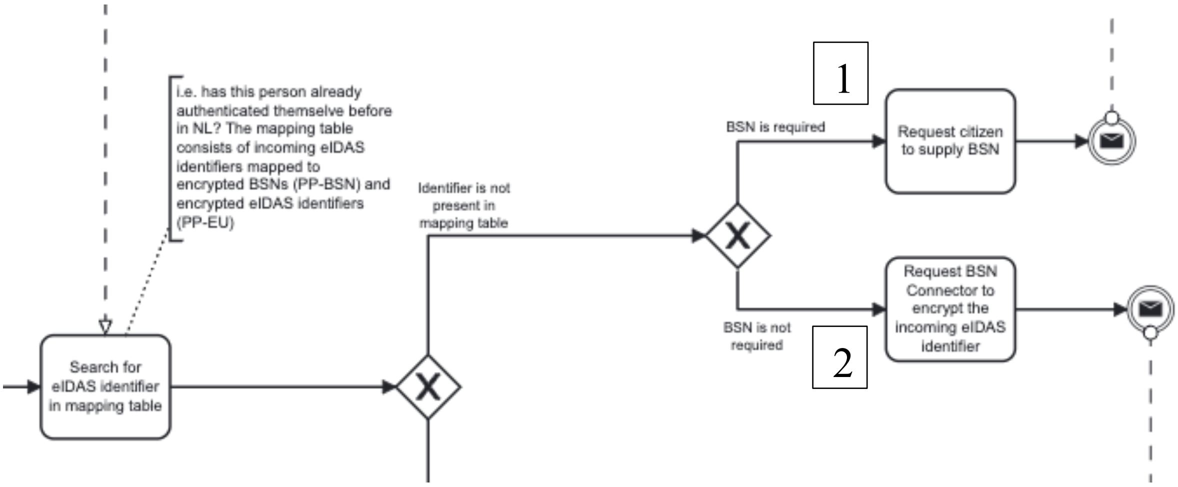

Figure 9: Steps when a new eIDAS identifier is received by the Dutch eIDAS Connector

If the incoming eIDAS identifier however is found in the mapping table of the eIDAS Connector, the eIDAS Connector will search if there is a RP-specific identifier (PP-RP) which corresponds to the RP where a citizen seeking to access services. If this PP-RP is found, it is sent to the RP. If this identifier is not found (i.e. this is the first instance where a citizen authenticates at this RP with an eID mean), one of the following two tasks are executed (visualized in figure 10):

1. **Identifier is found** in the mapping table & **BSN is required**: the encrypted BSN is sent to the BSN Connector. In this scenario, the citizen as already been linked to a BSN in a previous identification request. Therefore, the same encrypted BSN can be used again.

2. **Identifier is found** in the mapping table & **BSN is not required**: the encrypted eIDAS identifier (PP-EU) is sent to the BSN Connector.

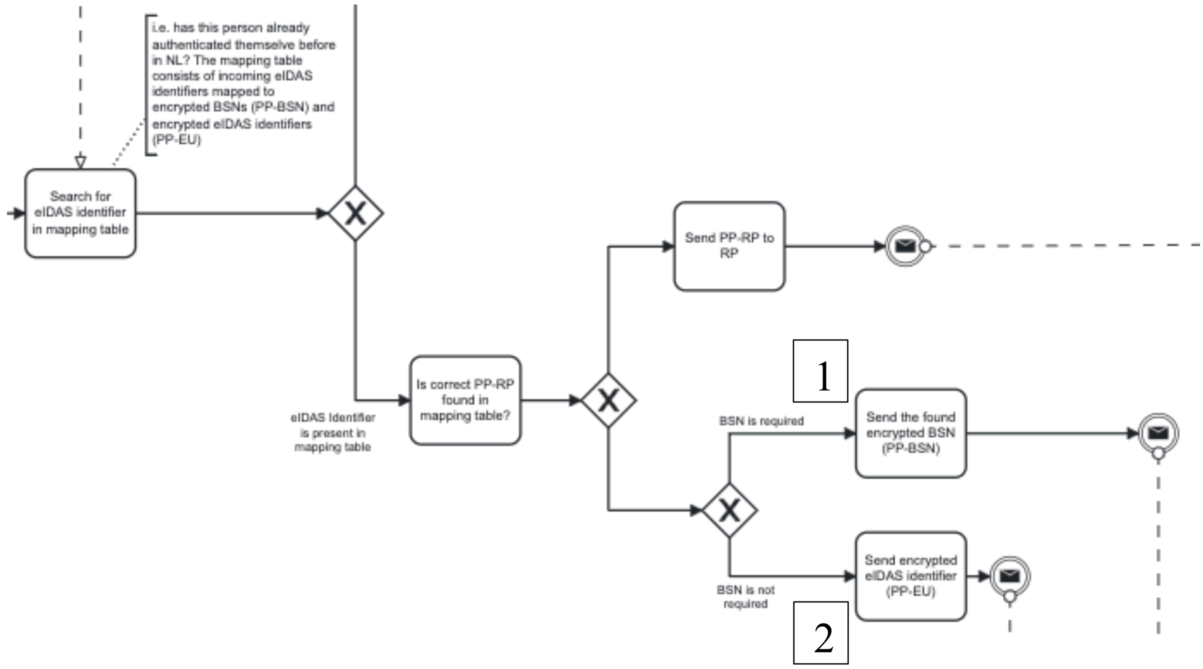

Figure 10: The eIDAS identifier is found in the mapping table of the eIDAS Connector.

Solely the first task results in attempt to match the incoming PID of the citizen with the BRP. Some of the previous tasks result in an identifier being sent the BSN connector for further encryption. The following explains the process flow after the first task (upper task of figure 9 and expanded in figure 11):

1. **Citizen is asked to supply BSN**: the citizen either returns a BSN or indicates that they do not know their BSN. In both cases, the citizen's name and date of birth is searched in the BRP by the BRP Connector. This results in four possible outcomes:

    a. **1 Match** is found & the citizen **has not** sent a BSN: the citizen is asked to confirm the last three digits of the found BSN. If the citizen rejects the last three digits, the citizen is denied access to the service and the process ends. If the citizen confirms the last two digits, there are two possible outcomes:

        i. If the PID **name matches** the BRP: the BSN is sent to the BSN Connector for encryption.

ii. If the PID **name does not match** the BRP: a government official will manually try to assess whether there is a match between the names in the PID and the BRP. The government official will be presented with records which have similarities with the incoming PID. These records are scored by how much they correspond to the PID. If a match is found, as in the former outcome, the BSN is sent to the BSN Connector for encryption. If a match cannot be found, the citizen is denied access to the service. Moreover, the eIDAS Connector is notified and the PID of the citizen is stored in the mapping table of the eIDAS Connector. This is done for two reasons (Interviewee 3, personal communication, July 6, 2022): Firstly, if the citizen seeks identification later with the same attributes, the manual search might be easier since the government official searching a match already knows the result of the previous matching attempt. Secondly, to be able to assess what caused a false negative match (a citizen is not matched, while there is a record of this citizen) in case a citizen files a complaint.

b. **More than one match** is found (irrespectively if the citizen has sent a BSN or not): a government official will manually try to assess whether the PID of the citizen matches one of the found records in the BRP. If no match is found, the citizen is denied access to the service. If one match is found: the BSN is sent to the BSN Connector for encryption.

c. **1 match** found & the citizen **has** provided a BSN: the BSN is sent to the BSN Connector for encryption.

d. **No match** found: the citizen is denied access to the service.

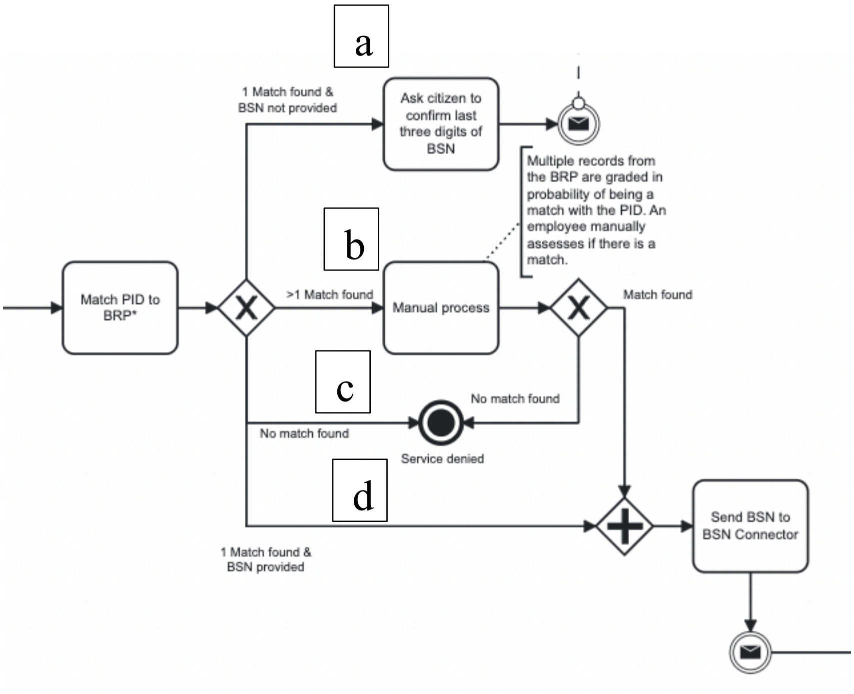

Figure 11: Matching the PID to the BRP

The process as described above has seen two possible outcomes:

- the citizen has been uniquely identified and an (encrypted) identifier has been sent to the BSN Connector for further encryption, or

- the citizen could not be uniquely identified and access to the service has been denied.

The BSN Connector can receive BSN, eIDAS identifier, or the encrypted version of these identifiers (PP-BSN or PP-EU respectively).

When the identifier has been encrypted into the correct form for the access rights of the RP, the BSN Connector encrypts the identifier into a PP-RP (identifier specifically for the RP in question). This identifier is made in three steps (figure 12). Firstly, the PP-CSN or PP-EU is randomized. Second, the randomized PP-CSN or PP-EU is encrypted with the public key of the RP. Lastly, this key is "reshuffled" in such a way that the BSN Connector does not have access to the outcome. The reshuffling is the metaphorical equivalent of "*shaking the vault"* (Verheul, 2019), the vault being the identifier encrypted with the RP's public key. Therefore, the BSN Connector and eIDAS Connector do not have access to the identifier which the RP receives. However, when the identifier is a PP-RP based on the CSN, and the RP decrypts this identifier, the eIDAS Connector and RP can communicate regarding this citizen, since both parties have the CSN. In the case of a PP-RP based on the eIDAS identifier, the eIDAS Connector and RP cannot communicate regarding this citizen, since the RP cannot decrypt this identifier to the same identifier which the eIDAS Connector holds.

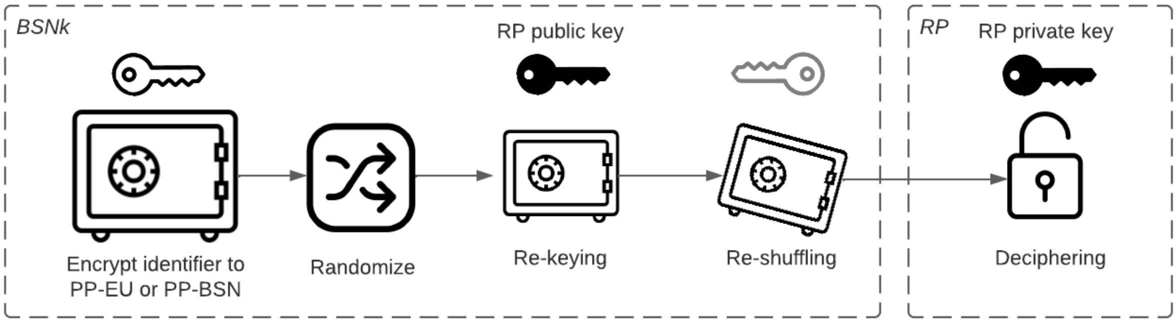

Figure 12: Encryption of PP-BSN and PP-BSN explanation (based on Verheul, 2019)

The BSN Connector sends the resulting identifier to the eIDAS Connector. The eIDAS Connector then saves this identifier in their mapping table and sends the RP specific identifier to the RP. The RP can trust the authenticity and integrity of the received identifier, because it is signed with the private key of BSN Connector. The Dutch government however does not give any guarantees on the uniqueness of the identifier sent (Interviewee 3, personal communication, July 6, 2022), since they encounter too many matching problems (elaborated in section 4.4). Therefore, a RP cannot trust that a citizen has not been assigned with an identifier which pertains to another citizen, or that a citizen has used another identifier at the RP in question in a previous identification attempt.

Hereafter, the following three situations can occur (figure 11):

1. The RP is allowed to see the original BSN for unique identification and can decrypt this BSN to match it to its database.

2. The RP is not allowed to see the BSN and is therefore given an identifier which it is not able to decrypt. It can use this identifier and PID to find a match in its database.

3. The RP only needs proof of an authenticated citizen, without establishing whether a pre-existing record of the citizen is present in their database (example of the speeding ticket photo) and can therefore grant the citizen access to the service after receiving the PP-RP (since the RP can trust the eIDAS network for the authentication process).

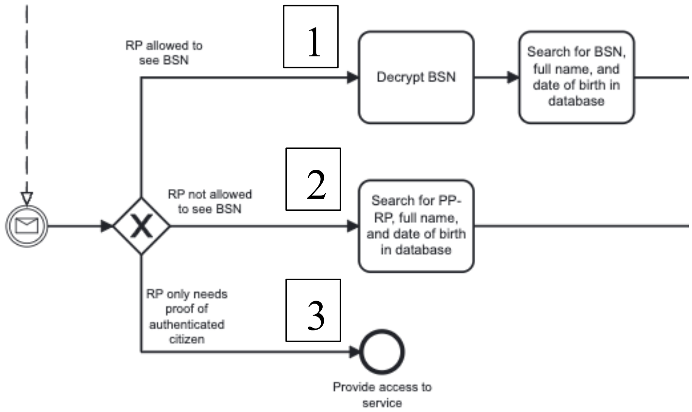

Figure 11: RP receives message from eIDAS Connector

The following steps in the process are an example of how a RP can match records to its database (visualized in figure 12). Since every RP has their own way of matching records, this process might not be applicable to each Dutch RP (Interviewee 3, personal communication, July 6, 2022).

1. One match is found with the provided identifier & the name provided in the PID matches the name in the records of the RP: provide citizen access to the service with the account that matches.

2. No match is found with the identifier: onboard citizen or deny access: depending on the context of the request. For example, if the request is to access certain medical records, an identifier not matching the record will result in a denial of access. However, a request for a new user account at will result in an onboarding process.

3. More than one match is found, or 1 match is found and the names do not match the records of the RP: try to manually match the citizen to a pre-existing record. If this results in one match: provide access to the service. If this does not result in a match, onboard citizen or deny access to service.

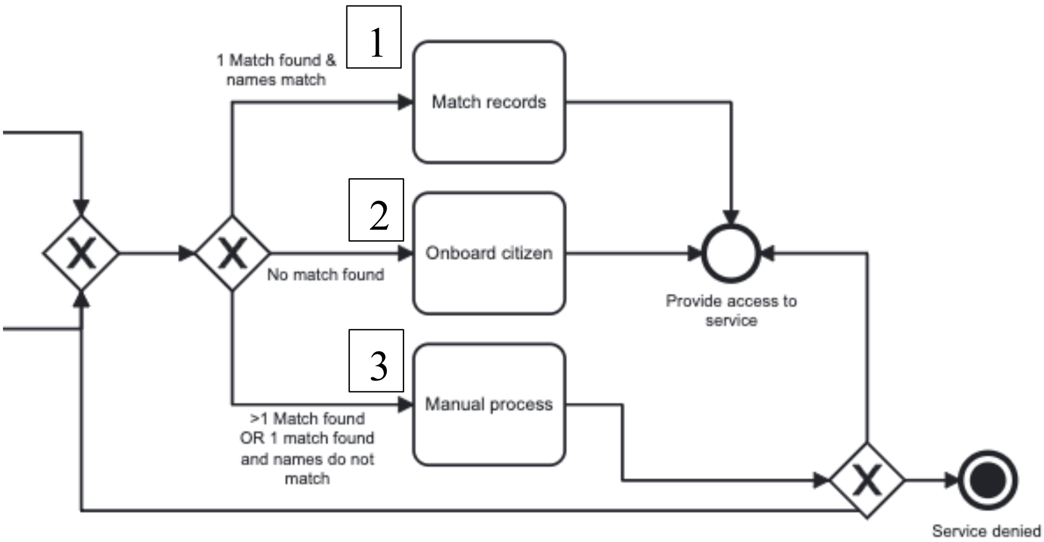

Figure 12: RP seeks match with citizen in records

4.3.4 Implications for Privacy and Reliability

The process organization of unique identification of citizens using foreign eID means has the following implications for privacy of citizens and the reliability of correct identification:

1. Each identification request depends on the eIDAS Connector, and first identification requests at a RP depend on the BSN Connector. Therefore, the eIDAS and BSN Connector are both a Single Point of Failure (SPOF).

2. The eIDAS Connector is a privacy hotspot because it has access to where each citizen authenticates themselves.

3. eID mean providers are privacy hotspots because they have access to which RP a citizen authenticates themselves.

4.4 Identity Management Theory

This section defines the current identity matching process along the terminology of identity management literature and states the implications of this definition on the privacy of citizens and the reliability of the matching process.

4.4.1 Identity Management

An identity can be described as "*a representation of an entity in a specific application domain*" (Jøsang & Pope, 2005). In this research, these entities are citizens. Identity management in this context can be described as the management of identities (e.g. pseudonyms) of a citizen. This entails the development of the identities and the choice of (re-) using these identities in a specific context or role (Pfitzmann & Hansen, 2010). An example of this is the creation of a pseudonym for a citizen which seeks identification at a tax office, which identifies that citizen in the context of the tax office. The party who can authenticate and attest attributes of a citizen is called an Identity Provider (IdP) (Chadwick, 2009).

The following describes four models of identity management, after which the current Dutch identity matching process is categorized in one of the four models.

4.4.2 Isolated Identity Management

In isolated identity management, service providers act as the providers of identity credentials (e.g. username and password) and RPs (figure 13) (Jøsang & Pope, 2005). This is a common model on the WWW, where citizens have different login credentials for different service providers (one username/password combination for Bol.com, another for Youtube.com, etc.).

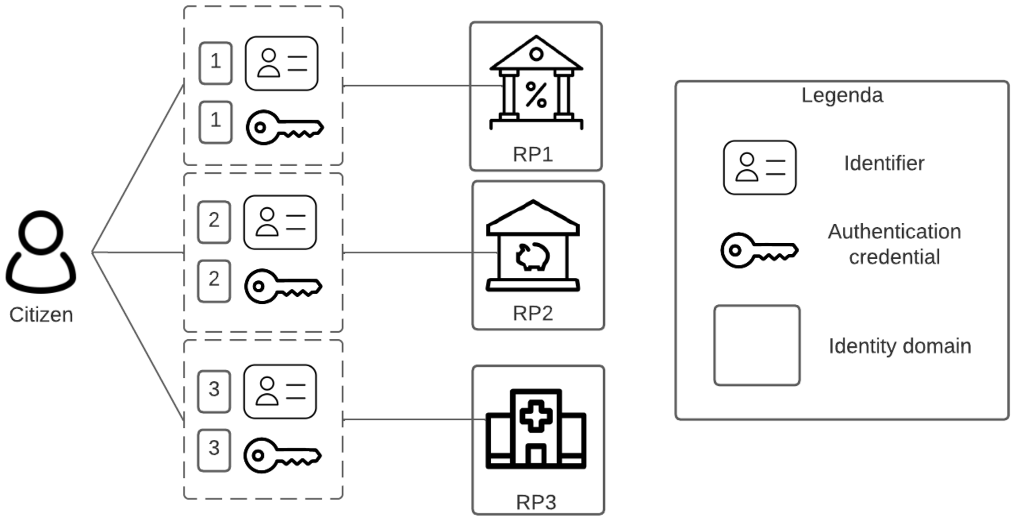

Figure 13: Isolated identity management model (based on Jøsang & Pope (2005))

4.4.4 Federated Identity Management

The isolated model is relatively simple for RPs to implement, but can be inconvenient for citizens, which must manage multiple username/password combinations. The federated identity management model seeks to counter this inefficiency through agreements within federations of RPs. An identity federation can be described as a group of RPs which recognize user identities and attributes which have been attested by other members of the group (figure 14) (Jøsang & Pope, 2005; Baldoni, 2012). This definition implies a certain trust between the RPs, which can be created through a set of agreements, standards, and technologies which enable the recognition of identities within the federation (Chadwick, 2009). A privacy issue in identity federations can be that citizens can be unaware of the exchange of information regarding themselves between RPs in the federation (Benantar, 2005). Moreover, by accumulating multiple identification requests of citizens at multiple RPs, it becomes possible to profile citizens (Hörbe & Hötzendorfer, 2015).

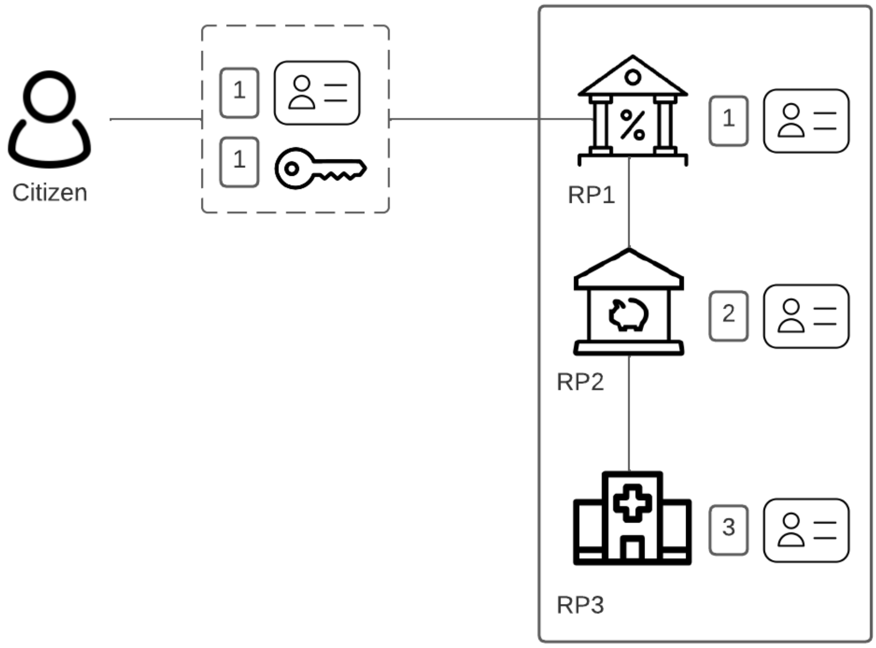

Figure 14: Federated identity management model (based on Jøsang & Pope (2005))

4.4.3 Central Identity Management

In a central identity management model, there is only one IdP which issues credentials which citizens can use at multiple RPs (Jøsang & Pope, 2005). It can be implemented in multiple ways. For this research, the meta-identifier model is the most applicable and will therefore be the only model described (figure 15). This central model contains one meta key of a citizen (e.g. a BSN), form which several credentials (e.g. pseudonyms and corresponding digital signatures) are derived which a citizen can use to authenticate themselves at a RP. The citizen therefore can identify themselves with one credential at multiple RPs.

This model is suitable for RPs which are managed by one organization (which is also the IdP), such as public bodies (where the government is the IdP) (Jøsang et al., 2007). The model is however less suitable for open environments due to privacy concerns. A centralized IdP ideally has access to as little personal information of citizens as possible. Having one central party aggregating identification requests across multiple domains is not desirable in the light of data minimization.

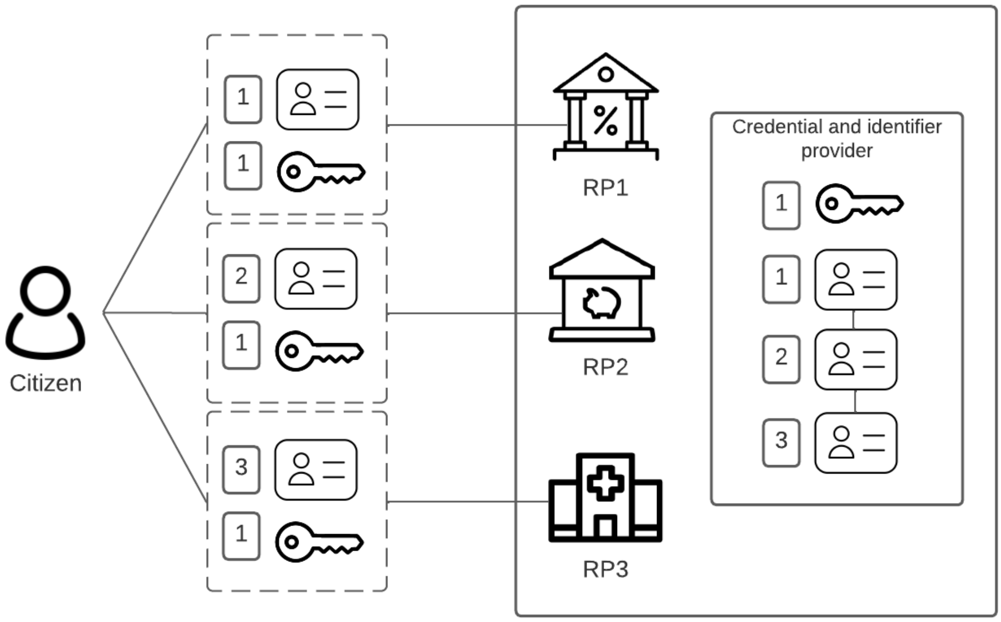

Figure 15: Central identity management model (based on Jøsang & Pope (2005))

4.4.5 User-centric Identity Management

The last identity management model covered is the user-centric model (figure 16) (Jøsang & Pope, 2005). This model seeks to give more control towards the user compared to the previous identity management model: the citizen has their identities and attributes stored on a personal device and can decide to share these with RPs. This gives the user more control over their personal information than the models described above, since there is no central party which stores all identities of a citizen and RPs are not able to recognize identities amongst each other without the user explicitly providing the same identifiers to multiple RPs. Moreover, the user only needs to remember/have the authentication method for the personal device, instead of having to do so for each RP.

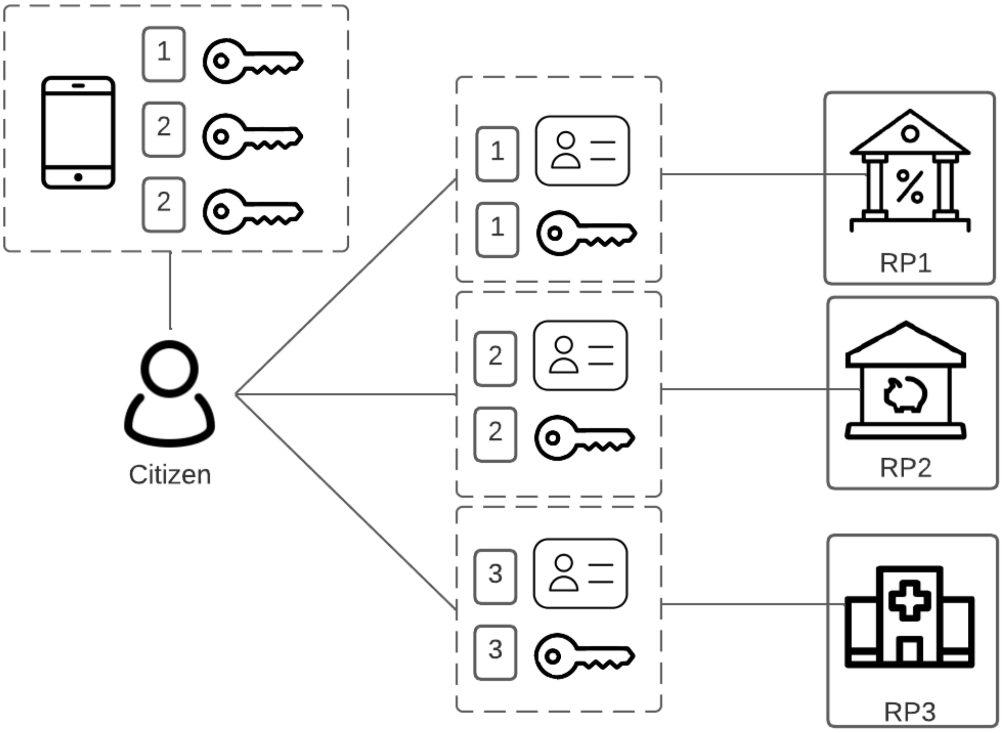

Figure 16: User-centric identity management model

4.4.6 Dutch Model Characterizations

An isolated model of identity management is not applicable to the Dutch identity matching process of foreign eID means since RPs do not act as identity providers in the current context. For example, the Dutch tax office (a RP) is not the same actor as the Dutch eIDAS and BSN Connector (IdPs). Moreover, a user can use one recognized eID mean to login to multiple RPs. There are however three similarities with the central meta user identity model as described by Jøsang and Pope (2005). First, identifiers used at service providers are provided by one central authority, Dutch eIDAS Connector. Second, there is communication between identity providers and RPs. Third, users have RP-specific identifiers.

The current situation however differs from the central model on the following three:

1. There are two meta-identifiers (eIDAS identifier and the CSN) from which the RP specific identifiers are derived.

2. The eIDAS identifier is not generated by the Dutch government, but by a foreign MS. Therefore, there are two IdPs instead of one.
3. Certain RPs can communicate amongst each other with one identifier (BSN) when they are authorized to do so, without the interference of the citizen or the IdP (Tax office and a bank communicating for detecting money laundering)

The latter aspect is a characteristic of the federated identity management model. Consequently, the current identity matching process of a foreign eID to a record at a Dutch public or regulated RP has characteristics of the central and hybrid identity management models. When analogously characterizing the eIDAS and BSN Connector as an IdP, the problems identified in the previous section (SPOF at the eIDAS/BSN Connector, privacy hotspots at eID mean providers and the eIDAS/BSN Connector) are also discussed in the literature describing the central and federated identity management models. To counter these problems, scholars point to more user-centric models (or incorporating user-centric aspects in federated models) to give, instead of IdPs and RPs, citizens more control over their personal information (Jøsang & Pope, 2005; Jøsang et al., 2007; Rieger, 2009; Slamanig et al., 2014). The eIDAS 2.0 regulation also seems to hint towards incorporating aspects of the user-centric identity management model, by stating that "*the user shall be in full control of the EUDI-Wallet*" (eIDAS 2.0, Recital 2 & 7, art. 6 sub a (7); Schwalm et al., 2022).

4.4.7 Implications of Characterization

The combination of the central and federated identity management models has the following implications for the privacy of citizens and the reliability of the process.

A privacy issue in identity federations can be that citizens can be unaware of the exchange of information regarding themselves between RPs in the federation (Benantar, 2005). Moreover, by accumulating multiple identification requests of citizens at multiple RPs, it becomes possible to profile citizens (Hörbe & Hötzendorfer, 2015).

The centralized model is suitable for RPs which are managed by one organization (which is also the IdP), such as public bodies (where the government is the IdP) (Jøsang et al., 2007). The model is however less suitable for open environments due to privacy concerns. A centralized IdP ideally has access to as little personal information of citizens as possible. Having one central party aggregating identification requests across multiple domains is not desirable in the light of data minimization. Since the EUDI-Wallet will also serve for uniquely identifying citizens in the private sector, the current identity matching process where the government is an IdP, and aggregates information of each identification attempt of a citizen.

4.5 Matching Reliability Problems

4.5.1 Reliability Problems

This section shows which reliability problems occur in the Dutch identity matching process.

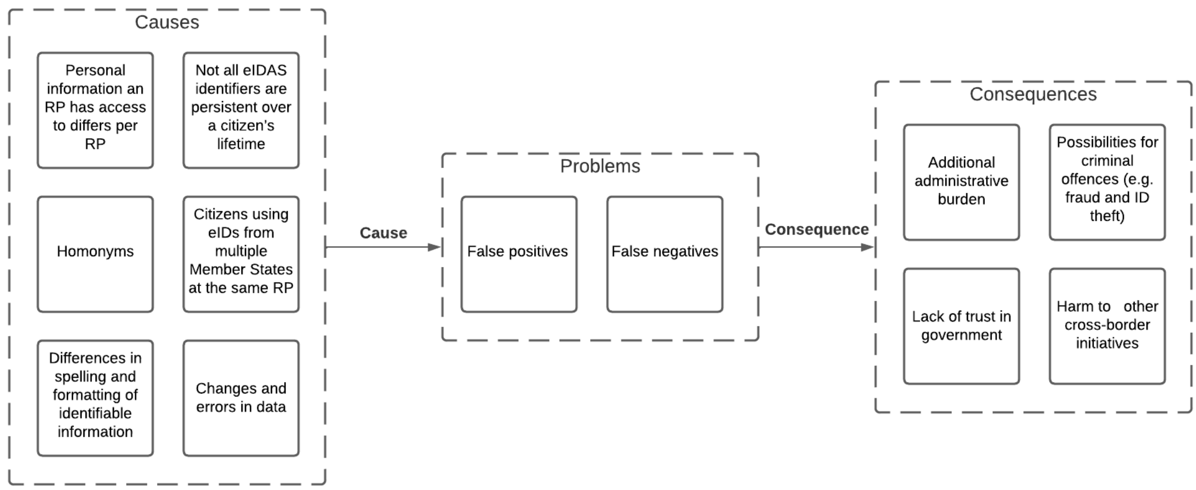

Figure 17: Summary of reliability problems found

The reliability problem in the identity matching process occurs when a citizen's PID cannot be uniquely linked to a record of that citizen in the BRP or the records of the RP where a citizen seeks authentication. The reliability problem can be divided into false positive and false negative matches. A false positive occurs when the RP or BRP Connector finds a match between a citizen which seeks authentication and a record of a citizen, while the record does not correspond to the citizen requesting authentication. A false negative occurs when a citizen is not matched to a record of that citizen, while the RP or BRP Connector holds the corresponding record. At onboarding, where there is no record of a citizen at a RP or BRP Connector, the only problem that can occur is a false positive. In subsequent matches, both false positives as false negatives can occur.

From a sample of 120 identity matching attempts of a foreign eID mean at the BRP Connector, 84 attempts (70%) lead to a correct match, 19 attempts (15.8%) do not match any record, and 17 attempts (14.2%) lead to one or more matches, but these do not correspond to the citizen identifying themselves (Interviewee 3, personal communication, July 6, 2022).

4.5.2 Causes

This section describes the causes for false positives and negatives in the current process of matching a foreign eID mean to a record of the BRP or of a Dutch public or regulated RP. A cause for false matches is that a RP identifies citizens in their records with a different identifier than they receive from the eIDAS Connector. This problem is not relevant for public service providers who are authorized to use the CSN as a unique identifier, since they can receive the CSN from the eIDAS Connector. Private service providers who are not allowed to process the CSN for unique identification must rely on the eIDAS identifier and a citizen's name and date of birth, which can change over time and can contain errors. A similar problem occurs at the BRP Connector when a citizen seeks authentication with an eID mean with different PID data than the citizen used at a previous authentication attempt. For instance due to name changes due to a divorce or marriage, differences in spelling of names and cities across MSs, errors in registries, and a different way of formatting birth and maiden names (Berbecaru et al., 2021; Krimmer et al., 2021a; Schmidt & Krimmer, 2022). Moreover, there are citizens of which their name and date of birth noted uniformly, but their name and date of birth is the same as that of another citizen.

Another issue is that the persistency of identifiers differs per MSs (Eurosmart, 2020; Schmidt et al., 2021). Some MSs (e.g. Estonia) provide citizens with only one unique and persistent eIDAS identifier, which remains unchanged regardless of the RP or the MS where the citizen seeks authentication. Other MSs (e.g. Germany) assign citizens a unique eIDAS identifier which is linked to the citizen's passport number. When a passport is renewed, the eIDAS identifier changes. Due to the problems associated with matching data which is possible not correct or up-to-date, the lack of identifier persistency can cause matching problems.

Another reliability problem can occur when a citizen of two MSs uses eIDs from both countries (with different eIDAS identifiers, and possibly also differences in the spelling of names) to identify themselves at a RP. In this situation, the RP has a record of the citizen with the first eID and must match that with the eID which uses a different identifier. Since the two identifiers are different, and therefore do not result in a match, other information of the citizen from the PID (i.e. full name and date of birth) must be used to match the citizen to a record. Due to for instance changes or errors in a citizen's identification data, it is possible that this data also does not result in a correct match between the citizen and its record.

4.5.3 Consequences

A false negative or false positive can lead citizens not being able to access services which require unique identification, since they cannot be identified. Moreover, false negatives and false positives can lead to an additional administrative burden, since more data of the citizen is needed to ensure a correct match, a match needs to be found manually, or the citizen needs to apply for (Berbecaru et al., 2021). Moreover, it can open the door for criminal offences such as fraud: if a citizen can intentionally accomplish false positives or negatives, the citizen can for instance apply multiple times for social benefits. This can have a negative effect on the trust of citizens have in their (national) government, whilst also harming other cross-border initiatives such as the Once-Only Principle (OOP) (Hinsberg et al. 2021; Schmidt et al., 2021). The OOP aims at ensuring that citizens only once need to provide necessary personal data to access governmental services.

4.5.4 Found Solution Directions

In literature and expert interviews, four solution directions have been named for the described reliability problems. Two are related to knowledge sharing between MSs and two are related to reliability requirements.

The solution suggestions regarding the sharing of knowledge are to leverage knowledge from similar cross-border initiatives such as the Single Digital Gateway Regulation, and for MSs to share information amongst each other regarding the problems they face in finding reliable matches.

The first reliability solution is to share more data regarding a citizen from trusted national sources for the purposes of unique identification (Leosk et al., 2017; Berbecaru et al., 2021; Schmidt & Krimmer, 2022). Considering the principle of data minimization it is however desirable to limit the amount of data sharing for the purposes of unique identification to a minimum.

The second functional solution is to further align identifier schemes and attributes amongst MSs (Berbecaru et al., 2021; Schmidt et al., 2021; Schmidt & Krimmer, 2022), as to decrease the chance of incorrect matches based on for instance differences in spelling between MSs. In the alignment of identifier schemes, two solutions are proposed. One is to oblige every MS to issue only one unique and persistent identifier for each citizen for the purpose of unique identification. There is however political resistance on the European proposition to introduce such an identifier (Commissiedebat Nr. 938, 2022) due to concerns related to profiling of citizens and its efficiency in solving the problem. Using only one unique and persistent identifier for each citizen at each RP they seek identification makes it trivial to link information about identifiable citizens, since a citizen would leave a unique number at each identification request. Due to the political resistance against such an identifier it is likely that the identity matching solutions will support the use of multiple unique and persistent identifiers per citizen. Moreover, only one unique identifier per citizen for cross-border use is unlawful in some MSs, such as Germany (WG3, 2022).

Besides the unlikeliness of one unique and persistent identifier being used per citizen under eIDAS 2.0, it does not necessarily benefit the identity matching process. For example, if a non-Dutch citizen seeks identification at a Dutch RP for the first time, this identifier is not present in the Dutch national registry (since the identifier is assigned by a foreign MS). The identifier alone is therefore not suitable for finding a match in the national registry. Therefore, additional data (for instance name, date of birth) which might be present in the national registry are necessary to be able to assess whether this citizen is present in the national registry. ensure that this citizen is uniquely identified. For future identifications, the unique identifier could be re-used. This however does not differ from the current Dutch identity matching process, where a citizen can have one identifier per RP.

4.6 Chapter Conclusion

This chapter answers the second sub-question:

Which privacy and reliability problems arise in the process of uniquely identifying a foreign citizen using an EUDI-Wallet to identify themselves at a Dutch regulated or public RP?

The process organization of unique identification of citizens using foreign eID means has the following implications for privacy of citizens:

1. The eIDAS Connector is a privacy hotspot because it has access to where each citizen authenticates themselves. Moreover, when a CSN is required for unique identification, the eIDAS Connector and the RP can communicate regarding that citizen.

2. eID mean providers are privacy hotspots because they have access to which RP a citizen authenticates themselves.

These privacy problems are also discussed in the literature describing the central and federated identity management models. Literature identifies the threat of a citizen not being aware how their personal data is processed, and the threat of having a privacy hotspot which spans multiple domains (i.e. public and private domains, such as is the case with the EUDI-Wallet).

To counter these problems, scholars point to more user-centric models (or incorporating user-centric aspects in federated models) to give, instead of IdPs and RPs, citizens more control over their personal information.

The reliability problems of the identity matching process are:

1. A citizen's PID not being uniquely linked to a record of that citizen in the BRP or the records of the RP where a citizen seeks authentication.

2. Each identification request depending on the eIDAS and the BSN Connector, which make the eIDAS and BSN Connector a SPOF.

The first reliability problem can be divided into false positive and false negative matches: there is a match between a citizen which seeks authentication and a record of that citizen, while the record does not correspond to the citizen requesting authentication, or a citizen is not matched to a record of that citizen, while the RP or BRP Connector holds the corresponding record.

To counter this reliability problem, literature and experts suggest leveraging knowledge from similar cross-border initiatives such as the Single Digital Gateway Regulation, and for MSs to share information amongst each other regarding the problems they face in finding reliable matches. Moreover, it is suggested to share more data regarding a citizen from trusted national sources for the purposes of unique identification and to further align identifier schemes and attributes amongst MSs. Shifting towards a more user-centric identity management model could counter the problem of the eIDAS and BSN Connectors being a SPOF.

Current literature and practice lacks solution directions which take the proposed amendment of the eIDAS regulation into account. Moreover, there is not a set of requirements regarding the privacy of citizens and reliability of finding a correct match which a solution direction must fulfill.

Chapter 5: Solution Directions for the Identity Matching Problems

5.1 Introduction

This chapter proposes three solution directions for the identity matching problems related to privacy and reliability as defined in the problem statement in the introduction of this research. To this end, firstly, the requirements a solution should meet and the constraints it is bound to are set out. Possible solution directions are explained thereafter, together with the extent to which the solution directions match the requirements is reviewed. Lastly, the benefits and barriers which experts have identified for the solution directions are discussed. This chapter thereby composes answers to the following sub-questions:

SQ2: *Which solution directions can be taken to solve the identified problems and meet the requirements of the Dutch Ministry of the Interior for uniquely identifying a citizen using a foreign EUDI-Wallet to identify themselves at a Dutch regulated or public RP?*

SQ3: *Which benefits and barriers do experts expect for the acceptance of a solution direction?*

The solution directions are visualized using BPMN models, since this modeling notation offers the possibility to model inter-organizational processes (Recker, 2008). Moreover, it allows exception flows, which is useful for different kinds of identification requests (e.g. identification with a BSN, or with an eIDAS identifier). The BPMN models describe which data regarding a citizen is transferred to actors of the Dutch government and a RP. The solution directions also describe which data regarding a citizen is accessible for an actor, and which data is not accessible to an actor due to encryption. This is done to show the privacy requirements are addressed in the solution directions. For the same reason, the solution directions also describe how access rights of RPs regarding personal data of citizens are assessed.

The process designs are limited to identification requests by EUDI-Wallets issued by MSs other than the Netherlands. Moreover, the way in which citizens authenticate themselves to the EUDI-Wallet is left out of the scope of this research (e.g. username and password, biometrics). Information which is not in the PID dataset is left out of scope for the issue of linkability of information to citizens. It is for instance not considered how browser activity and IP-addresses can be used to identify a user by an adversary. Different roles a citizen may take, such as acting on behalf of another citizen or legal person, is also left out of scope. The solution directions also do not cover the agreements between MSs regarding the reliability and privacy of unique identification, and how these should be reached to obtain their go

The following two assumptions are made based on the eIDAS 2.0 Regulation's text:

- There will be a EUDI-Wallet
- Unique identification of citizens will be established through their PID.

5.2 Requirements, and Constraints

5.2.1 Constraints

The constraints are conditions which must be met for any solution direction. The reliability constraints consist of agreements which MSs should come to which are necessary for any possible solution to work. As mentioned in section 5.1, agreements between MSs on the persistency of identifiers and attribute (formats) is not in the scope of the solution directions and will therefore not be elaborated in the solution directions. Likewise, the privacy constraints contain legislative acts related to privacy which each solution should meet.

5.2.1.1 Reliability Constraints

RC1 **An identifier must not be assigned to more than one citizen.** In the current eIDAS 1.0 process, subsequent identifications solely depend on matching two identifiers. If an identifier can relate to more than one citizen, it is not possible to trust the uniqueness of an identifier (Interviewee 1, personal communication, July 1, 2022).

RC2 **The (combination of) identification data must be enough to uniquely identify a citizen within the records of the BRP or of a Dutch public or regulated RP.** The current eIDAS minimum dataset is not sufficient to ensure unique identification of citizens across the EU (when a commonly known identifier is not provided). This is because the minimum data set does not guarantee unique identification in each MS, and data in the data sets can be subject to changes (e.g. name change). MSs do not know if the attributes which can optionally be requested by other MSs ensure unique identification. Moreover, the optional attributes are not always aligned with the attributes of the requesting MS (e.g. Spain can share an e-mail address as an optional attribute, but this attribute is not present in the Dutch national registry). To be able to match incoming attributes with a data set, MSs must know which attributes are being sent and which attributes are available in their data sets (Berbecaru et al., 2021; Interviewee 1, personal communication, July 1, 2022; Interviewee 3, personal communication, July 6, 2022).

RC3 **Data which is shared to ensure unique identification must be noted in a single format (e.g. date of birth as dd/mm/yyyy)** (Interviewee 1, personal communication, July 1, 2022; Interviewee 3, personal communication, July 6, 2022; Berbecaru et al., 2021).

RC4 **The notation of diacritics and punctuation marks which are shared to ensure unique identification must be uniform across all MSs (e.g. the notation of an ü, notation of maiden names with and '-')** (Interviewee 3, personal communication, July 6, 2022).

RC5 **The translation of data which is shared to ensure unique identification must be uniform across all MSs (e.g. between different languages and scripts)** (Interviewee 3, personal communication, July 6, 2022).

5.2.1.2 Privacy Constraints

PC1 **Personal data must be accurate and, where necessary, kept up to date (**GDPR, art. 5 (1d)).

PC2 **Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.** **(**GDPR, art. 5 (1b))

PC3 **Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed** (GDPR, art. 5 (1e)).

PC4 **Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject (**GDPR, art. 5 (1a)).

PC5 **The citizen must have given consent to the processing of his or her personal data for one or more specific purposes (**GDPR, art. 6 (1a)).

PC6 **Appropriate technical and organizational measures (e.g. pseudonymization) must be implemented which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing (**GDPR art. 25 (1)).

5.2.2 Requirements

This section contains the requirements which the solution directions should meet to satisfy the needs of the Dutch Ministry of the Interior. Therefore, these are requirements for the ministry.

The reliability requirements are what a solution requires to solve the reliability problems:

1. A citizen's PID not being uniquely linked to a record of that citizen in the BRP or the records of the RP where a citizen seeks authentication.

2. Each identification request depending on the eIDAS and the BSN Connector, which make the eIDAS and BSN Connector a SPOF.

5.2.2.1 Reliability Requirements

RR1 **A regulated or public Dutch RP must be able to assess whether a citizen authenticating themselves has a pre-existing record at that RP if this is necessary for the provision of their services, regardless of the home MS of that citizen.** Practitioners have stated in interviews that they would accept an error rate, since errors in citizen registries are inevitable (Interviewee 1, personal communication, July 1, 2022; Interviewee 3, personal communication, July 6, 2022). A specific error rate was not given (European Commission, Recital 17, art. 11a (1), 2021).

RR2 **For identification at a Dutch public or regulated RP which is allowed to process the BSN for the purpose of unique identification, the Dutch government must first be able to assess whether the citizen authenticating themselves has a pre-existing record in the BRP.** RPs in the public sector who are allowed to process the BSN of citizens depend on the BSN for unique identification. Instead of having each RP matching PID data with their own records to find the corresponding citizen and its CSN, it is desirable to have a central service do this for these RPs. This is based on two reasons. Firstly because RPs do not have the necessary means in place to match PID data to their records. Secondly because a central service bundles knowledge on errors of incoming eID means. This means that the matching algorithm can be improved easily. Thirdly, because it can reduce the total implementation costs (costs for the government + costs for RPs), since only one service needs to implement a sophisticated identity matching functionality, instead of each Dutch RP (Interviewee 2, personal communication, July 4, 2022; Interviewee 3, personal communication, July 6, 2022).

RR3 **A regulated or public Dutch RP must be able to assess the authenticity of an identifier of a citizen which it is intended to receive.** A RP needs to be able to assess whether the identifier came from the citizen it pertains to.

RR4 **A regulated or public Dutch RP must be able to assess the integrity of an identifier of a citizen which it is intended to receive.** An adversary should be able to tamper with identifiers.

RR5 **A citizen must only be able to use one identifier per regulated or public Dutch RP for the purposes of unique identification.** For RPs to be able to trust in the uniqueness of identifiers, a citizen should not be able to use multiple identifiers to represent him/herself (Verheul, 2019; Interviewee 1, personal communication, July 1, 2022).

RR6 **A regulated or public RP must be able to uniquely identify a citizen without an intervention of the Dutch government.** The identity matching process should eliminate the SPOF at the Dutch government.

The privacy requirements are what the Dutch Ministry requires to solve the privacy problems related to the current process of uniquely identifying a citizen.

1. The eIDAS Connector is a privacy hotspot because it has access to where each citizen authenticates themselves.

2. eID mean providers are privacy hotspots because they have access to which RP a citizen authenticates themselves.

The second problem is not addressed by the requirements, because not giving EUDI-Wallet providers access to where a citizen authenticates themselves creates a privacy legislation issue.

It is undetermined whether an EUDI-Wallet provider is to be considered a processor of personal data as defined in the GDPR (art. 4 para 7 GDPR). Under eIDAS 1.0, if an eID mean provider provides services which use the BSN to uniquely identify citizens, they are seen as a processor of personal data as defined in the GDPR (art. 4 para 7; Authenticatiedienst als verwerker van het BSN, 2022). If the EUDI-Wallet provider is a processor of personal data as defined in the GDPR (art. 4 para 7), the EUDI-Wallet provider must be able to prove that the citizen has given consent to share their personal information with a certain RP (art. 15 & 28 GDPR; Verheul, 2019). This is not possible without keeping a record of the RPs where a user has authenticated themselves. For this research, it is assumed that EUDI-Wallet providers are processors of personal data regarding the identifiers which are sent to a RP, and therefore need to be able to prove with which parties these identifiers are shared.

5.2.2.2 Privacy Requirements

PR1 **Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (e.g. data minimization)** GDPR art. 5 (1c), eIDAS 2 Recital 29 and art. 6(a) sub 7, (Tsakalakis et al., 2018).

PR2 **Dutch RPs must not be supplied with a citizen's BSN for identification purposes, unless they are required to by national (sectoral) legislation such as the Wabb and WBSN-Z.** These regulations regulate RPs that are allowed to process the BSN of citizens for the purpose of unique identification (Wabb art. 10).

PR3 **No one must be able to assess whether an encrypted BSN and eIDAS identifier correspond to the same citizen.** Linkability concerns the possibility of someone being able to link two items of interest together. These items can for instance be two logs of authentication requests of a citizen. If it is trivial to link many items, it is possible to create profiles of citizens Linkability is seen as unauthorized when there is no legal obligation for it. The linkability of citizens should be limited to what is necessary to uniquely identify citizens for the purposes of the eIDAS 2.0 Regulation or other Union or national laws (such as AMLD5). (Wuyts & Joosen, 2015; Tsakalakis et al., 2018).

PR4 **An EUDI-Wallet provider must not have access to the BSN of a citizen.** Since the EUDI-Wallet can be developed by a private party, which in principle are not allowed to process a citizen's BSN, EUDI-Wallet providers should not have access to the BSN of a citizen (Wabb art. 10; eIDAS 2.0 art. 6(a) sub 7).

PR5 **The provider of the EUDI-Wallet provider must not be able to see the identifier which the citizen uses to identify themselves at a RP.** To remove the privacy hotspot which is currently located at the providers of eID means.

PR6 **Encrypted RP-specific identifiers which are not meant to be decryptable, must not be decryptable by any RP.** An adversary should not be able to know if two identifiers which are intended for a RP relate to the same person. Moreover, if an encrypted RP-specific BSN instead of a RP-specific eIDAS identifier is sent to a RP by mistake, the

RP must not be able to decrypt the identifier in such a way that the BSN becomes accessible. Moreover, it gives citizen's more insight in which parties can uniquely identify them. This is desirable since citizens run the risk of not knowing what happens to their personal data in a federated identity management model (Benantar, 2005).

PR7 **Encrypted RP-specific which are not meant to be decryptable, are not decryptable by any RP.** Identifiability means that the items of interest as mentioned in PR3 can be linked to an identifiable citizen. Identifiability is seen as unauthorized when there is no legal obligation for identifying a citizen (Wuyts & Joosen, 2015). The identifiability of citizens should be limited to what is necessary to uniquely identify citizens for the purposes of the eIDAS 2.0 Regulation or other Union or national laws (such as AMLD5).

PR8 **The Dutch government must not have access to the identification requests of a citizen.** It is not desirable that the government as IdP has access to where a citizen identifies themselves across multiple domains since it opens possibilities to profile citizens (Jøsang et al., 2007; Hörbe & Hötzendorfer, 2015).

5.3 Solution Directions

5.3.1 Labeling of Processes

The solution directions discussed in this section for the identity matching problems are named the government-centric, hybrid, and wallet provider-centric. The extent to which the citizen's EUDI-Wallet provider takes over the responsibilities which under eIDAS 1.0 lie at the Dutch government (i.e. creating identifiers and checking access rights of RPs) is the main divisor for the three solution directions. The reason for this axis is that, as identified in the literature review (4.3), eIDAS 2.0 seems to move from a central/federated approach to identity management towards a more user-centric approach. By designing and evaluating three processes which vary in degrees between the more central/federated and user-centric approach, it becomes clearer what the implications are of the degree of re-using the current way of organizing the process of identity matching. These solution directions do not represent all possible means to tackle the identity matching problems. For instance, using a secure mobile component on a citizen's smartphone for creating identifiers is not present in any of the discussed solution directions. Since limiting the linkability and identifiability of citizens are required to solve the (PR1 & PR2), all solution directions support the use of multiple identifiers. The solution directions are visualized BPMN diagrams. Lastly, the extent to which each architype fulfills the requirements for a solution is set out in Appendix D, and the morphological charts which show different options for a set of functions for the solution directions are located in Appendix E.

5.3.2 Solution Descriptions

5.3.2.1 Government-centric Solution Direction Approach

Figure 18 illustrates a simplified version of the government-centric approach. The eIDAS, BSN, and BRP Connector are merged in the 'Dutch government' swimming pool. The full process model can be consulted at: https://antonwelling.nl/identity-matching-central-approach/

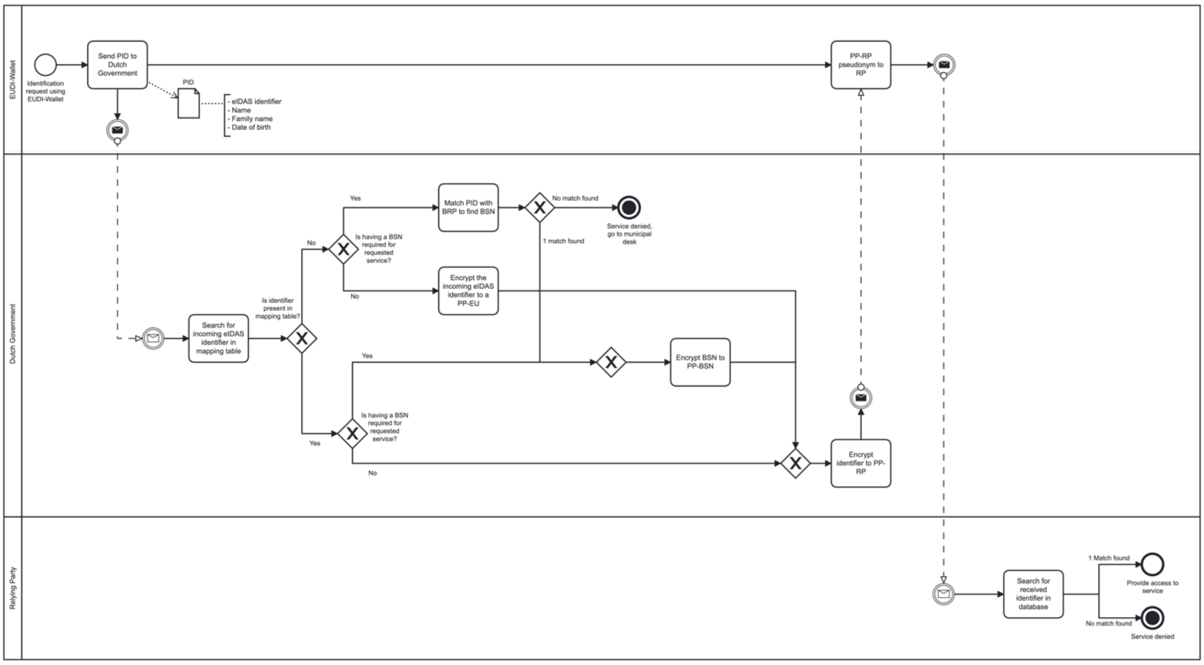

Figure 18: Government-centric approach to identity matching

In the government-centric approach, citizens are uniquely identified by the Dutch Ministry of the Interior, the Dutch Ministry of Economic Affairs, and the RP. The eIDAS Connector determines the level of identity matching necessary for the service requested (i.e. unique identification with a BSN, or with an eIDAS identifier). The government-centric solution direction resembles the current Dutch eIDAS 1.0 identity matching process. Because this process described in section 4.3, the following is limited to the differences between the two approaches.

In the government-centric approach, the non-Dutch eIDAS nodes have no role in the identity matching process. Where in eIDAS 1.0 these nodes send the PID to the Dutch eIDAS Connector, it is now the citizen who sends their PID from their wallet to the Dutch eIDAS Connector. This prevents the eIDAS node of the foreign MS from overseeing the citizens identification attempts.

In the Dutch eIDAS 1.0 process, the BSN Connector would send the RP-specific identifier (PP-RP) to the Dutch eIDAS Connector, which then sends it to the RP. In the government-centric approach, the eIDAS Connector sends the RP-specific identifier to the citizen. The citizen then sends this identifier to the RP. This change avoids communication between the Dutch government and the RP, since this prevents the government from knowing at which point in time a citizen authenticates themselves at a RP. Moreover, sending the identifier to the EUDI-Wallet of the citizen, instead of to the EUDI-Wallet provider, the EUDI-Wallet provider does not have access to the identifier which a citizen uses to identify at a RP (thereby meeting PR5). Because the eIDAS Connector needs to be consulted for each identification request, thereby leaving each identification request known to this party, the data minimization requirement is not met (PR1). Due to the eIDAS Connector having access to each identification request of a citizen, as well as the identifier which a citizen uses to uniquely identify at a RP, PR8 (Dutch government must not have access to identification requests) is also not met.

A central party can be practical for identity matching since it bundles knowledge and experience of previous identity matching problems. The more experience a party has with matching identities, the better it can anticipate on future anomalies (such as differences in data formats from data coming from other MSs) (Interviewee 3, personal communication, July 6, 2022). This centrality however also creates a SPOF where identity attributes of all citizens are handled: if one of the functions fails (e.g. the eIDAS connector), there is no other component which can ensure unique identification. Due to this SPOF, the government-centric solution does not meet RR6.

Evaluation

Experts labeled the extent of reuse of existing infrastructure as a benefit to the government-centric approach. According to them, the reuse could facilitate the transition of eIDAS 1.0 to eIDAS 2.0 since little adaptations of the current identity matching process need to be altered. The matches with foreign eID means which have already been made in eIDAS 1.0 do not need to be redone. Moreover, the existing way of checking the access rights of RPs can remain intact (contrarily to the hybrid and wallet provider-centric approach, which propose a new method). Another expected benefit is that MSs and foreign EUDI-Wallet providers are not required to implement a polymorphous encryption system such as the Netherlands and can continue with their system of creating identifiers as they have under eIDAS 1.0. The current centralized approach allows for the Dutch government to access identification requests of a citizen. This facilitates the back-office communication between competent authorities regarding a citizen, which can be useful for use cases such as tax reporting or fraud detection, in which case banks and tax offices must be able to uniquely identify a citizen. Another benefit mentioned is that the government-centric approach is likely to lead towards a user-friendly process, since the identity matching process at the Dutch government needs to be fulfilled once, after which subsequent matches will mostly be trivial (provided the RP in question is allowed to use the BSN for the purpose of unique identification).

The SPOF at the Dutch eIDAS Connector is expected to be a barrier for accepting the government-centric approach: each identification request (a citizen’s first, as well as subsequent identifications) is processed by this actor. Therefore, no identification requests are possible when the eIDAS Connector fails. The need for the eIDAS Connector relates to another expected barrier: the dependency on online availability. It is possible that the EUDI-Wallet will also need to accommodate identification requests without being able to connect to a central service. It is therefore perceived as a barrier that all identification requests flow through the Dutch eIDAS Connector. Lastly, since all identification requests are accessible by the Dutch eIDAS Connector, experts expect that the government-centric approach can lead to possibilities for unnecessary/unlawful tracking of the personal data and activities of citizens.

Besides benefits and barriers, points to consider regarding the solution direction were asked during the evaluation. Experts mentioned that it would be beneficial if the solution could reuse matches which have been made under eIDAS 1.0 so that these do not become obsolete. Another point mentioned was to use attestations of correct matches instead of identifiers. After onboarding, a citizen could receive an attestation of a successful match by the Dutch government and save this in their wallet. This attestation could then be shared with a RP. This could solve the privacy hotspot issue which currently lies at the Dutch government, which consists of a mapping table with all identifiers which a citizen has shared with a RP. Moreover, the obligation of a citizen to retrieve a new identifier from the Dutch government for each RP it seeks identification with could cause potential extra steps in the user flow, which could lead to a process which is less user-friendly than other solution directions. Another point to consider is the cost model behind the public key infrastructure. In the government-centric approach, the Dutch government handles the encryption of identifiers. It is possible that many private services will make use of this service after eIDAS 2.0 goes into effect. Therefore, it is important to consider how the costs of setting up and maintaining infrastructure such as a public key registry are allocated.

Table 3: Summary of the evaluation of the government-centric solution direction

Expected Benefits	Expected Barriers	Points to Consider
Reuse of infrastructure	Single Point of Failure (SPOF)	Attestations instead of consecutive matches
Standardization	Dependency on online availability	Cost model
Reuse of (back-office) data	Unnecessary tracking of citizens	Reuse of infrastructure
Centralization		Privacy hotspot at IdP
User-friendly (positive)		User-unfriendly

5.3.2.2 Hybrid Solution Direction

Figure 19 illustrates a simplified version of the hybrid approach. The full process can be consulted at: https://antonwelling.nl/identity-matching-hybrid-approach/

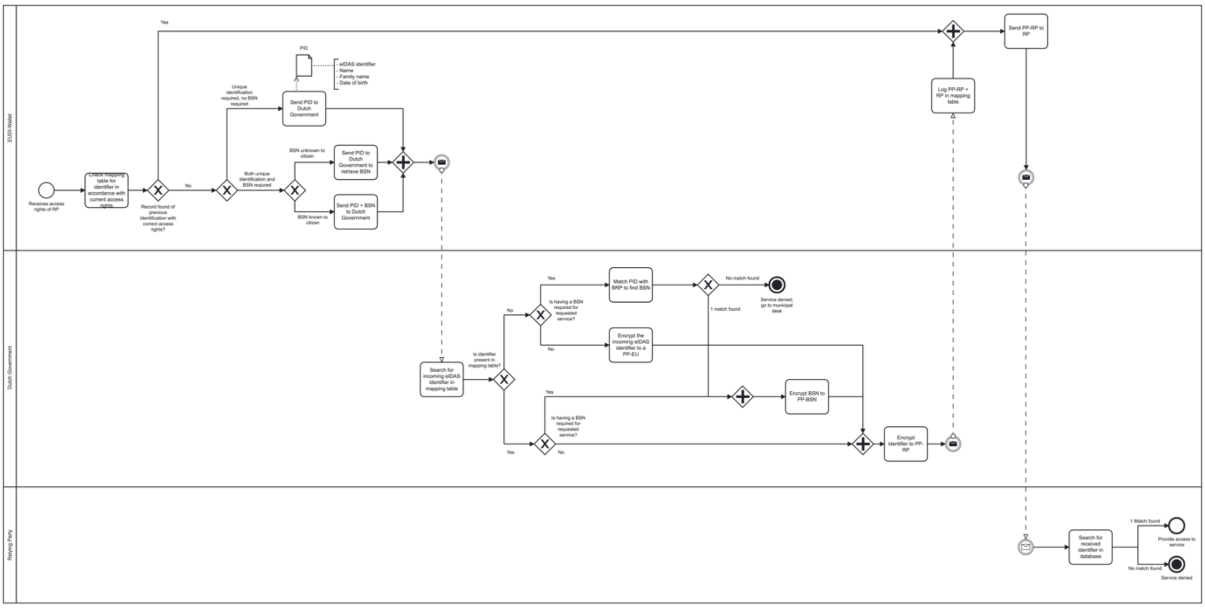

Figure 19: Hybrid approach to identity matching

Contrarily to the government-centric approach, besides the Dutch government and RP, the citizen also plays a role in matching identities in the hybrid approach. The two differences in the hybrid approach to the government-centric approach are that the citizen checks the access rights of the RP (i.e. which identifier the RP is allowed to use for identification purposes) and keeps a mapping table of previously used identifiers. Due to these differences, the BSN and eIDAS Connector do not have access to subsequent identification requests of a citizen.

When a citizen requests authentication at a RP, the RP shares which identifier they have the right to access to the citizen through a verifiable credential. The citizen's EUDI-Wallet then proceeds to verify the access rights of the RP. If some form of unique identification is required, the EUDI-Wallet of the citizen checks whether the mapping table in the EUDI-Wallet (stored locally on a citizen's smartphone) contains an identifier of a previous identification at the RP in question (i.e. is there a PP-RP of the RP). If this identifier is present in the mapping table, this identifier is sent to the RP. Because the identifier contains a signed certificate of the BSN Connector, the RP can trust the authenticity and integrity of the identifier.

If the identifier is not present in the mapping table, the citizen requests the Dutch eIDAS connector for the necessary identifier. To this end, the citizen sends it's PID, along with the access rights and identity of the RP (and the identity of the RP) in question. The eIDAS connector is solely requested to retrieve the necessary identifier, not to assess whether a RP has the correct access rights, since this is already assessed by the citizen. After the EUDI-Wallet receives the PP-RP of the eIDAS Connector, it is saved locally in the mapping table of the EUDI-Wallet for subsequent identification requests at the RP in question. By sending the PP-RP directly to the RP for subsequent identification requests, a citizen can identify themselves directly at a RP for subsequent identification requests without the interference of the Dutch government. The process of uniquely identifying a citizen at a RP is the same as in the eIDAS 1.0 process.

The eIDAS Connector also keeps a mapping table of previously issued PP-RPs as in the government-centric approach. The benefit of this is that the citizen can retrieve their mapping table of previously used PP-RPs from the eIDAS Connector when they lose possession of their EUDI-Wallet.

By being necessary for each first identification request at a RP, the hybrid solution direction does not meet PR8 (Dutch government does not have access to identification requests of the citizen) and RR6 (no intervention from Dutch government needed for identification requests).

Evaluation

An expected benefit of the hybrid (as with the government-centric) approach is that the current identity matching process at the Dutch BSN and eIDAS Connector is left intact. This ensures that citizens can be uniquely identified in the Dutch national registry, as well as the current process of creating identifiers can remain the same. Another benefit shared with the government centric approach is that MSs and foreign EUDI-Wallet providers are not required to implement a polymorphous encryption system. Moreover, the hybrid approach is expected to limit the tracking of citizens by the Dutch government compared to the government-centric approach: subsequent identification requests at a RP are not detectable by the Dutch government since the citizen sends the PP-RP directly to the RP. The Dutch eIDAS and BSN Connector however can see every RP where a citizen seeks unique identification. This is expected to be a barrier for accepting the solution, since solely the knowledge of where a citizen identifies themselves can pose a considerable privacy infringement for the citizen (e.g. logging into a psychiatric consultation).

Another expected barrier is the SPOF at the Dutch BSN and eIDAS Connector. If it fails, no new identifiers can be created. Subsequent identification requests however can be made, since the EUDI-Wallet can handle these identification requests directly with the RP. The consequences of the SPOF are therefore less severe than with the government-centric approach. Moreover, there is still a dependency on online availability since new identifiers need to be retrieved from the BSN Connector.

A point named to consider when choosing the hybrid solution direction is that it requires additional logic requirements for the EUDI-Wallet, since the wallet needs to be able to assess the access rights of RPs. Moreover, RPs need to be able to share verifiable information on their access rights to citizens. This is expected to increase the implementation effort and could therefore become a barrier for acceptance. Moreover, checking the access rights of RPs could lead to potential extra steps in the user flow, which could lead to a less user-friendly process. Another point raised is to consider is that citizens might have the option use multiple identifiers at one RP to authenticate themselves, thereby using their service under multiple pseudonyms (e.g. create multiple twitter accounts, act in representation of another natural/legal person). If this is required, the solution should be able to accommodate this.

Table 4: Summary of the evaluation of the hybrid approach

Expected Benefits	**Expected Barriers**	**Points to Consider**
Reuse of infrastructure	Unnecessary tracking of citizens	Additional logic requirements needed of wallet
Standardization	SPOF	Different levels of identity matching (identify/authenticate)
Allows tracking of citizens when necessary	Dependency on online availability	User friendliness (negative)

5.3.2.3 Wallet Provider-centric Solution Direction

Figure 20 illustrates a simplified version of the onboarding wallet provider-centric approach, and figure 21 illustrates the process for identification attempts at Dutch RPs. The full process can be consulted at: https://antonwelling.nl/identity-matching-decentral-approach/

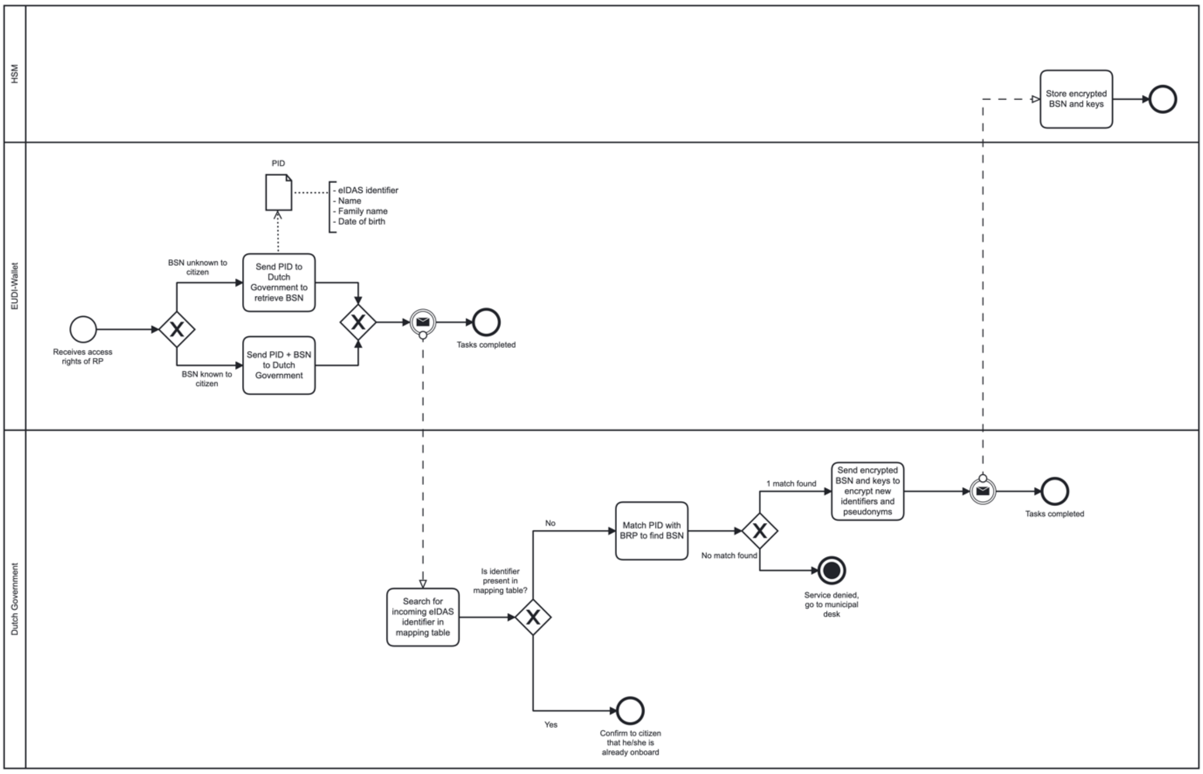

Figure 20: Onboarding the EUDI-Wallet for identification requests at Dutch RPs

The wallet provider-centric identity matching process resembles the hybrid identity matching process. The difference between the approaches is that, instead of the BSN Connector, a Hardware Security Module (HSM)* located at the EUDI-Wallet provider is used to encrypt identifiers. The HSM ensures that cryptographic keys are not available outside the HSM in plain text. Moreover, the HSM contains logic which permits the keys to only be used in a predefined way (Verheul, 2019). Due to this decision, the EUDI-Wallet only needs the eIDAS and BSN Connector for the onboarding process of the wallet (as visualized in figure 20). The BSN Connector is only needed to supply the HSM with the necessary cryptographic material to generate identifiers as if the HSM were the BSN Connector. After onboarding, the eIDAS and BSN Connector do not need to be consulted for identifications at Dutch RPs (whether they are first or subsequent identification requests) (visualized in figure 21). This removes the SPOF that these actors form in the current process of uniquely identifying a foreign eID mean.

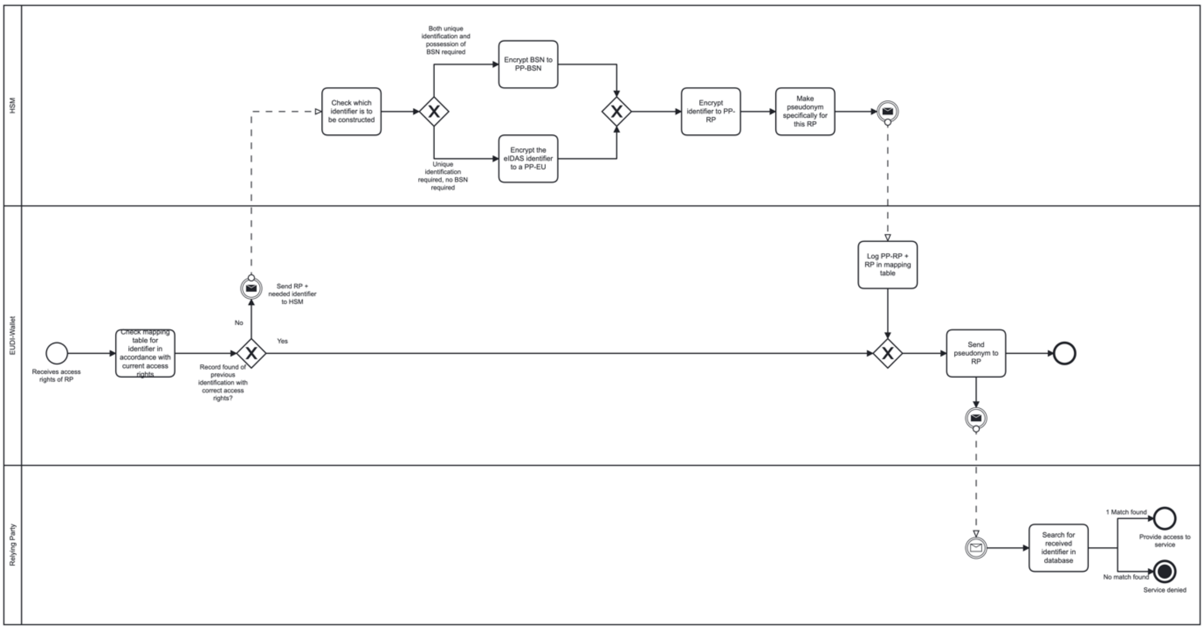

Figure 21: Identification requests with the wallet provider-centric approach after onboarding

As with the hybrid identity matching process, the citizen's EUDI-Wallet determines the level of identity matching needed and can send the corresponding identifier (PP-RP) directly to the RP if this is present in the wallet's mapping table. As with the hybrid process, the citizen's wallet contains a mapping table of previous identification requests and the identifiers used. This prevents the HSM at the EUDI-Wallet provider from being necessary for each subsequent identification request at a RP. Upon receiving the identifier, the RP can then proceed to uniquely identify the citizen in their records as in the other solution directions. As with the other solution directions, the PP-RP contains a signed certificate from the BSN Connector (through the initial key pair), proving the authenticity and integrity of the identifier.

Since the mapping table of the citizen's identifiers is located only on the citizen's EUDI-Wallet, loss of the wallet results in a loss of the mapping table. However, due to the uniqueness and persistency of a citizen's BSN and the RP's public key, the HSM can create new PP-RPs which are identical to those in the lost mapping table.

Evaluation

An expected benefit of the wallet provider-centric approach identified by experts is that it offers citizens more privacy and control regarding the tracking of their identification requests by the Dutch government in comparison to the other approaches. Due to the HSM located at the EUDI-Wallet provider, the Dutch government does not know at which RPs a citizen authenticates themselves. Since one of the propositions of the eIDAS 2.0 regulation is to give more control to citizens regarding their personal data, this approach was expected to be the easiest of the three to communicate to the public. The last benefit mentioned is that this solution direction (compared to the government-centric and hybrid) depends the least on one central service: the HSMs are spread at the providers of EUDI-Wallets. This benefit was mentioned with the remark that it only holds true when there are multiple providers of EUDI-Wallets. This was expected to have a positive effect on the scalability of wallet use, since the number of identification requests is not constrained by the capacity of one central service. Again, under the assumption of there being multiple EUDI-Wallet providers.

An expected barrier mentioned for the wallet provider-centric approach is that it requires the EUDI-Wallet provider to know at which RPs a citizen seeks identification. Experts state that it should be explored whether there is a possibility to avoid this. Another expected barrier mentioned is the implementation costs for MSs and RPs to communicate with the wallet, as well as the complex logic which should be added to the wallets. The additional logic relates to the checking of access rights of RPs (same as with the hybrid approach) and the creation of identifiers by the EUDI-Wallet provider.

A point raised to consider regarding the wallet provider-centric solution is if it allows for the legitimate tracking of citizens by the Dutch government or authorized RPs. In some situations, RPs and the Dutch government are allowed to link information of one citizen which can be located at multiple RPs (e.g. tax and bank information in a money laundering investigation). Due to the identifiers being created at the HSM, neither the Dutch government nor the EUDI-Wallet provider have access to the identifiers which are shared with a RP. Another point to consider is that in the current solution, loss of the wallet (e.g. due to loss of the phone which carries the wallet application) means loss of the mapping table which contains the identifiers which a citizen used per RP. Upon losing the wallet, the identifiers which a citizen used to communicate with a RP need to be constructed again. These new identifiers are however the same as the ones on the lost wallet since these are constructed with the private key of the citizen and the public key of the RP, which both remain unchanged (Verheul, 2019).

Another point raised to consider is that the citizen would have more control over their identifiers if they were created on a personal device of the citizen instead of at the EUDI-Wallet provider. This point was accompanied by the remark that there should be a mechanism which prevents the citizen from being able to use multiple identifiers at the same RP. The last point raised to consider questions the added value of using polymorphic pseudonyms compared to regular pseudonyms.

Table 5: Summary of the evaluation of the wallet provider-centric approach

Expected Benefits	**Expected Barriers**	**Points to Consider**
Less tracking of citizens by Dutch government	Tracking of citizens (privacy hotspot at HSM)	Legitimate tracking possible?
Easy to communicate to the public	Large investments	Does loss of wallet mean loss of the mapping table?
Continuity and scalability	Additional logic requirements needed of wallet	More control over identifiers. Maybe create identifiers within wallet
Least dependency on central services	Dependency on online availability	Why Polymorphic Pseudonyms

5.4 Evaluation

5.4.1 Introduction

This section first shows the patterns, inferences, and tradeoffs drawn from the evaluation of the solution directions and how these relate to literature on identity management. Second, a possible choice of tradeoffs is proposed which is in line with the stance the Dutch Ministry of the Interior takes in official publications. The tradeoffs are only applicable to the solution directions as described in the previous section. There can be solution directions where these tradeoffs are averted.

Table 6: Technical benefits and barriers

Technical	**Government-centric**	**Hybrid**	**Wallet provider-centric**
Benefits			
Reuse of (back) office data	x		
Barriers			
Dependency on online availability	x	x	x
SPOF	x	x	
Additional logic requirements needed of wallet			x

Table 7: Organizational benefits and barriers

Organizational	**Government-centric**	**Hybrid**	**Wallet provider-centric**
Benefits			
Reuse of infrastructure	x	x	
Centralization	x		
Standardization	x	x	
Continuity and scalability			x
Least dependency on central services			x
Barriers			
Large investments			x

Table 8: External environment benefits and barriers

External Environment	**Government-centric**	**Hybrid**	**Wallet provider-centric**
Benefits			
User-friendliness	x		
Tracking of citizens		x	x
Easy to communicate to the public			x
Barriers			
Tracking of citizens	x	x	x

5.4.2 Evaluation Conclusions

The outcome of this evaluation is categorized in the technical, organizational, and external environment context of the Dutch identity matching process (tables 6, 7, and 8). The technical scope concerns variables related to the functions of the wallet and of the identity matching service. The organizational scope relates to the governance and the division of responsibilities in the identity matching process. The external environment relates to the interests of citizens (e.g. privacy) and the relationship with actors outside of the Netherlands.

Each solution direction is evaluated by experts which identified benefits, barriers, and points to consider further for each solution direction. Another interesting outcome is that tracking of citizens is seen an issue in each solution direction. However, the hybrid and wallet provider-centric solution directions have been identified as offering benefits to counter the tracking of citizens over the government-centric solution direction, since subsequent identification requests are not visible for the Dutch government.

Each solution direction has been labeled as having a dependency on online availability, since all contain the need to connect to the eIDAS Connector and/or the EUDI-Wallet provider for identification requests. The wallet provider-centric solution direction is however the only one which has not been identified during the focus group as having a SPOF. In the wallet provider-centric solution direction, identification requests do not depend on the eIDAS Connector: they depend on the citizen's EUDI-Wallet provider. Assuming that there will be multiple EUDI-Wallet providers, from the perspective of the system, there are multiple points of failure. From a citizen's perspective there however still is a SPOF, since the citizen depends on its EUDI-Wallet provider for first identification requests.

No organizational barriers have been raised during the focus group regarding the government-centric and hybrid solution directions. This could be due to the similarities between the process of identity matching under eIDAS 1.0 and the process as proposed in the government-centric and hybrid solution direction. The wallet provider-centric solution direction does have barriers related to the organizational context, which consequently could be because the process organization differs more from the current organization than the other two approaches. This conclusion is supported by the fact that both the government-centric and hybrid solution directions have been named the benefits of standardization and the reuse of infrastructure, while the wallet provider-centric solution direction was not given these benefits. Moreover, large investments to change the current process organization have been named a barrier for the wallet provider-centric solution direction.

The hybrid approach has two benefits corresponding with the government-centric approach, namely standardization and the reuse of infrastructure. The government-centric solution direction further has benefits related to the reuse of (back-) office data and centralization. The wallet provider-centric approach has no benefit which is present in the central approach, and vice versa. The hybrid solution direction shares benefits and barriers with the government-centric and wallet provider-centric solution directions. This could have been foreseen due to the hybrid solution being a combination of two opposites.

Another interesting observation is that the government-centric approach's benefits are similar to the wallet provider-centric approach's barriers, and the government-centric approach's barriers are similar to the wallet provider-centric approach's benefits: the government-centric approach was assigned benefits such as the reuse of infrastructure and standardization, while the wallet provider-centric approach was assigned with barriers such as requiring large investments and demanding additional logic requirements of the wallet. The government-centric approach's barriers SPOF, dependency on online availability, and tracking of citizens seem to be addressed in the wallet provider-centric approach, which contains benefits related to giving more privacy and control to citizens, having a fit with offline use cases, and depending the least on central services compared to the hybrid and government-centric approach. This can be an indication of trade-offs which have to be made when choosing one of the three solution directions: no solution direction can counter the barriers of the other solution directions without acquiring new barriers which were accounted for in the other solution directions. According to Jøsang et al. (2007), tradeoffs are unavoidable when designing identity management solutions. Moreover, they state that infrastructure providers are inclined to opt for solutions which are advantageous to them, but do not necessarily benefit the user in terms of privacy. This inclination could eventually become problematic for both the user and the infrastructure provider.

Between the government-centric and wallet provider-centric solution directions, the following trade-offs are identified:

	Government-centric		**Wallet provider-centric**
T1	*Reuse of infrastructure and centralization at the cost of citizen privacy and control.*	***vs.***	*Privacy and control for citizens at the cost of large investments and additional logic requirements for the EUDI-Wallet.*
T2	***Reuse of infrastructure** and centralization at the cost of having a SPOF.*	***vs.***	***Less dependency on central services** at the cost of creating a privacy hotspot at the HSM (which is located at the EUDI-Wallet provider.)*

The reuse of the centralized infrastructure of the government-centric solution direction has been labeled as having a negative effect on the privacy of citizens, since the Dutch eIDAS Connector logs each identification request of a citizen. The wallet provider-centric approach counters this by making the eIDAS Connector 'blind' to these identification requests, but this comes at the cost of possibly large investments and additional logic requirements for the wallet. This is in line with the conclusion of Hörbe & Hötzendorfer (2015), which have found a positive correlation between the strength of controls limiting the tracking of citizens and their implementation effort in federated identity management systems. They state that a tradeoff must be made based on privacy risks, incentives, and costs.

The reuse of the centralized infrastructure also brings forth the issue of having a SPOF at the Dutch eIDAS Connector. The wallet provider-centric approach has less dependency on central governmental services but shifts this to a dependency on the EUDI-Wallet provider, which is responsible for the generation of identifiers, thereby shifting the privacy hotspot. T2 is also present between the hybrid and the wallet provider-centric solution directions. T1 is partially accounted for by the hybrid solution direction, due to there being privacy benefits of the hybrid compared to the government-centric solution direction. Moreover, the hybrid solution does not require HSMs to be placed at each EUDI-Wallet provider, which could lead to less investments needed compared to the wallet provider-centric solution direction. The hybrid solution direction has not been evaluated as having the barriers of requiring large investments and additional logic requirements of the wallet. In practice, additional logic requirements to the EUDI-Wallet will be needed, since the hybrid solution direction requires wallets to check the access rights of the RP, which the government-centric solution direction does not require. Therefore, the hybrid solution direction is not a flawless answer to the tradeoffs between the government-centric and wallet provider-centric solution direction.

5.4.3 Recommendations

Based on the privacy and reliability requirements, the wallet provider-centric solution direction is the most fitting choice of the three proposed solution directions. Tradeoffs must be made when opting for one of the proposed solution directions. This section provides arguments for why the choice for the wallet provider centric solution direction, compared to the government-centric and hybrid, is most in line with the stance of the Dutch Ministry of the Interior.

The Dutch Ministry of the Interior and the EU seek to provide citizens more privacy and control over their personal data (eIDAS 2.0, Recital 2 & 7, art. 6 sub a (7); Schwalm et al., 2022; VVD et al., 2022). Due to creating a privacy-friendly digital identity being a top priority (van Huffelen, 2022), it seems appropriate to place citizen privacy and control above the cost of large investments to achieve this (T1). The tradeoff between the reuse of infrastructure while having a SPOF, compared to less dependency on central services while creating a privacy hotspot at the HSM of the EUDI-Wallet provider (T2) is less straight forward. Having a SPOF for online identification does not fit within the objectives of the Dutch government (Verheul, 2019). The wallet provider-centric solution direction however does not solve this problem sufficiently since a citizen is dependent on the EUDI-Wallet provider instead of on the eIDAS and BSN Connector. The citizen is however not dependent on the EUDI-Wallet provider for subsequent identification requests, since for these requests the citizen can send the identification data directly to the RP. The problem of having a SPOF could be solved by design choices which are not described in the proposed solution directions. A secure mobile component on a citizen's smartphone could for instance be used for the generation of identifiers, thereby avoiding the need for consulting the BSN and eIDAS Connector and the EUDI-Wallet provider at each identification request. Not all citizens however possess a smartphone which contains a secure component, which could interfere with the objective of the ministry to give each citizen the possibility to use an EUDI-Wallet (van Huffelen, 2022).

The ambitious deadline for the implementation of the EUDI-Wallet set by the Commission for 2025 could make it difficult to implement a solution which necessitates a high implementation effort. Therefore, it might be difficult for the Ministry to implement wallet-centric or wallet provider-centric solution since this requires changing the current process significantly. More research should be done as to assess whether there is a solution direction which removes the SPOF, whilst also meeting the objectives of the Dutch Ministry of the Interior related to privacy and inclusiveness, whilst being implementable within the given deadline.

Chapter 6: Conclusion and Discussion

6.1 Conclusion

SQ1: *Which privacy and reliability problems arise in the process of uniquely identifying a citizen using a foreign EUDI-Wallet to identify themselves at a Dutch regulated or public RP?*

Under eIDAS 1.0, a citizen with a foreign eID mean seeking access to services of a Dutch regulated or public RP in the Netherlands is uniquely identified by the RP and a central service (Dutch eIDAS and BSN Connectors). This approach resembles characteristics of the central and federated identity management models as defined by Jøsang and Pope (2005). Through literature research and expert interviews, this research found discusses identity matching problems which relate to:

1. the reliability of a match, and
2. the privacy of citizens.

The process organization of unique identification of citizens using foreign eID means has the following implications for privacy of citizens:

1. The eIDAS Connector is a privacy hotspot because it has access to where each citizen authenticates themselves. Moreover, when a CSN is required for unique identification, the eIDAS Connector and the RP can communicate regarding that citizen.
2. eID mean providers are privacy hotspots because they have access to which RP a citizen authenticates themselves.

These privacy problems are also discussed in the literature describing the central and federated identity management models. To counter these problems, scholars point to more user-centric models (or incorporating user-centric aspects in federated models) to give, instead of IdPs and RPs, citizens more control over their personal information.

The reliability problems of the identity matching process are:

1. A citizen's PID not being uniquely linked to a record of that citizen in the BRP or the records of the RP where a citizen seeks authentication.

2. Each identification request depending on the eIDAS and the BSN Connector, which make the eIDAS and BSN Connector a SPOF.

SQ2: *Which solution directions can be taken to solve the identified problems and meet the requirements of the Dutch Ministry of the Interior for uniquely identifying a citizen using a foreign EUDI-Wallet to identify themselves at a Dutch regulated or public RP?*

The requirements for a solution to these problems are divided in privacy and reliability requirements. The two foremost reliability requirements for a solution are:

1. A regulated or public Dutch RP must be able to assess whether a citizen authenticating themselves has a pre-existing record at that RP if this is necessary for the provision of their services, regardless of the home MS of that citizen.

2. A regulated or public RP must be able to uniquely identify a citizen without an intervention of the Dutch government.

The privacy requirements set limits to the linkability of personal data and the identifiability of citizens. These are requirements such as PR6: encrypted RP-specific identifiers which are not meant to be decryptable, are not decryptable by any RP.

The three solution directions for the privacy and reliability problems are labeled the government-centric, hybrid, and wallet provider-centric approaches. The extent to which the citizen's wallet (provider) takes over the responsibilities which under eIDAS 1.0 lie at the Dutch government (i.e. creating identifiers and checking access rights of RPs) is the main divisor for the three processes. The government-centric approach does not meet the requirements of data minimization (PR1), avoiding intervention the Dutch government (RR6), and avoiding the Dutch government from having access to each identification request (PR8). The hybrid approach does not meet RR6 and PR8. The wallet provider-centric solution direction is the only proposed approach which meets all requirements of the Dutch Ministry of the interior.

SQ3: *Which benefits and barriers do experts expect for the acceptance of a solution direction?*

In two focus groups, each solution direction is evaluated by experts. These experts identified benefits, barriers, and points to consider further for each solution direction. The outcome of this evaluation is categorized in the technical, organizational, and external environment context of the Dutch identity matching process.

In the technical context, the government-centric approach has been accredited with the benefit of reusing (back) office data such as previous matches of the eIDAS Connector. Each solution direction has been identified as having a dependency on online availability, because the first identification requests always depend on either the BSN and eIDAS Connector or the EUDI-Wallet provider. The government-centric and hybrid solution directions have been identified as having a SPOF. The wallet provider-centric approach has been identified as requiring additional logic requirements from the wallet.

The government-centric and hybrid solution directions offer no barriers in the organizational context, which could be due to the similarities between the process of identity matching under eIDAS 1.0 and the process as proposed in the government-centric and hybrid solution direction. Both the government-centric and hybrid approaches have been identified as having the benefit of reusing existing infrastructure. The wallet provider-centric solution direction does have a barrier related to the organizational context (large investments), which consequently could be because the process organization differs more from the current organization than the other two approaches. Besides reusing infrastructure, the government-centric approach has also been identified as having the benefits of centralization and standardization.

In the external environment context, tracking of citizens is an issue in each solution direction. Contrarily to the government-centric solution direction, the hybrid and wallet provider-centric have been identified as offering benefits to counter the tracking of citizens, since subsequent identification requests are not visible for the Dutch government. The wallet provider-centric solution direction is accredited with being easy to communicate to the public. The government-centric solution direction is identified as being user-friendly.

Tradeoffs have been identified between the government-centric and wallet provider-centric solution directions: no solution direction can counter the barriers of the other solution directions without acquiring new barriers which were accounted for in the other solution directions. These tradeoffs are:

	Government-centric		Wallet provider-centric
T1	*Reuse of infrastructure and centralization at the cost of citizen privacy and control.*	***vs.***	*Privacy and control for citizens at the cost of large investments and additional logic requirements for the EUDI-Wallet.*
T2	*Reuse of infrastructure and centralization at the cost of having a SPOF.*	***vs.***	*Less dependency on central services at the cost of creating a privacy hotspot at the HSM (which is located at the EUDI-Wallet provider.)*

The hybrid solution direction does offer an answer to the tradeoffs by partly reusing the current identity matching process, while offering more privacy to citizens than the government-centric solution direction. However, the hybrid approach still requires additional logic requirements form the EUDI-Wallet and more investments compared to the government-centric solution direction. It is therefore not a flawless answer to the tradeoffs between the government-centric and wallet provider-centric solution directions.

The main research question of this research is:

Which solution directions can be taken to meet the requirements of the Dutch Ministry of the Interior for solving the privacy and reliability problems related to uniquely identifying a citizen using a foreign EUDI-Wallet to identify themselves at a Dutch regulated or public RP?

This research proposes three solution directions which can be taken to solve the privacy and reliability related to uniquely identifying a foreign citizen using an EUDI-Wallet to identify themselves at a Dutch regulated or public RP. The wallet provider-centric solution direction is the only approach which meets all requirements, while the government-centric and hybrid respectively do not meet three and two requirements. Due to the aim of the EU and the Dutch Ministry of the Interior to give citizens more privacy and control over their personal data, the wallet provider-centric solution direction seems the most desirable direction of the three. More research should be done as to assess whether there is a solution direction which removes the SPOF, whilst also meeting the objectives of the Dutch Ministry of the Interior related to privacy and inclusiveness and is implementable within the given deadline. If there is no solution which meets these criteria, research should be done to what solution is feasible within the given deadline, together with a roadmap on how to achieve the desired solution in later iterations.

6.2 Discussion

6.2.1 Interpretations and Implications

There are four aspects of this research which contribute to the decision-making process of the Dutch Ministry of the Interior for choosing a solution direction. First, the description of the privacy and reliability problems related to matching a foreign eID mean to a record at public and regulated Dutch RPs, together with its causes and consequences. Secondly through the elicitation of what the Dutch Ministry of the Interior requires to solve the privacy and reliability problems. Third by providing three evaluated solution directions which, either partially or fully, satisfy the Ministry's requirements. Lastly, advice is given for a solution direction which fits within the Ministry's policy stances.

Besides the Dutch government, the research offers practical contributions for other MSs who are designing a solution for EUDI-Wallet requests. The problem description contains problems related to the matching of foreign eID means, which is relevant for each MS, since the eIDAS regulation applies to the whole EU. MSs can also use the research as an inspiration for a solution direction which is aligned with their needs regarding privacy and reliability (which might differ from those of the Dutch Ministry of the Interior). Moreover, for MSs who currently use a central identity matching service provider by their government, the solution directions can serve as an inspiration for the implications of the transition from their current government-centric identity matching process to a more EUDI-Wallet provider-centric process.

For Dutch public and regulated RPs the solution directions and options in the morphological charts can give an insight in the different ways the identity matching process of foreign EUDI-Wallets may be organized. RPs can use these insights to determine which option is the most desirable for them and to communicate this to the Dutch Ministry of the Interior through one of their stakeholder communication channels.

The scientific contribution of this research is threefold**.** Firstly the research gives a description of the identity matching problems related to reliability and privacy elicited from literature and expert interviews. Secondly in the possible solution directions and morphological charts give an overview of the possible solution directions which the Dutch Ministry of the Interior can take to solve the reliability and privacy problems. Such an encompassing description of problems and solution directions related to identity matching is not present in academic articles to date. Further, the solution directions add to the development on reusable theories on what avenues can be taken to solve privacy and reliability problems related to identity matching. Lastly, the research shows the similarities between existing identity management research, and how these theories can give guidance for choosing a solution direction for identity matching problems related to reliability and privacy. This is the first research which applies these theories to the identity matching problems related to privacy and reliability of the proposed EUDI-Wallet. It is also the first research in context of identity matching which combines design science research and the TOE model to design solution directions and draw inferences on the evaluation of experts.

6.2.2 Limitations

Regarding the privacy requirements, linkability caused by other meta-data and digital footprints besides the identifiers mentioned in this research have not been considered. Due to advancements in data analytics, seemingly anonymous data can still be used to uniquely identify a citizen.

The approaches are to be seen as a starting point because they seek to solve a constantly evolving problem: new exception cases are still being discovered, the process of identity matching under eIDAS 2.0 is not set in stone, and the Dutch Ministry of the Interior has not taken an official stance on multiple architectural decisions. Moreover, new requirements may appear in the legislative process which is still underway (for instance on how RPs are registered, and how their access rights are determined). This could cause a solution direction to not be compliant anymore with the eIDAS 2.0 regulation.

It is important to note that Dutch EUDI-Wallet identification request (both nationally and cross-border) have not been considered in the designs. While the process could possibly flow in a similar way, there can be requirements for this which have not been foreseen in this research. Moreover, how the citizen authenticates themselves to the wallet (e.g. with biometrics, username/password, two factor authentication), and the Level of Assurance (LoA)* at which EUDI-Wallets will be onboarded have not been covered in this research. These are important aspects in the overall process, since it determines the level of which a RP can be sure the citizen seeking identification is who they say they are. Moreover, citizens acting on behalf of other citizens or legal persons have not been considered. These are relevant topics regarding the stimulation of the internal market and the adoption of the EUDI-Wallet. Lastly, identification requests where the wallet has no internet connection have also not been considered. This is however important for use cases such as mobile driver licenses.

Regarding the evaluation of the processes, it is important to consider that there might be more benefits and barriers to these solution directions than have been elicited. Moreover, the benefits and barriers that are mentioned are what the participants expect to occur and have been subject to the interpretation of the researcher. The (interpretation of) expected benefits and barriers might not be aligned with practice since the solution directions have not been implemented at the time of evaluation. Therefore, there might be more benefits, barriers, and tradeoffs than mentioned in this research. Moreover, since the solution directions are not implemented in practice, there is a risk of a more positive evaluation than when these would be implemented.

Since the scope of this research does not allow for every solution direction being explored, there might be solution directions which have not been considered which are more desirable for the Dutch Ministry of the Interior than the solution directions proposed.

6.2.3 Recommendations

The extent to which certain variables form a benefit or barrier for acceptance of a solution have not been empirically researched. This research gives a starting point for such an empirical study by listing the variables which experts have identified to evaluate solution directions.

Besides an empirical analysis on the influence of variables, more research can be done regarding the impact the solution directions have on the viability of the cost sharing model of the EUDI-Wallet. The solution directions vary in the financial costs they bring forth (e.g. setting up PKI). The wallet might be provided by a private party, and there might be a vast number of private RPs. It is therefore important that a decision is made on how these costs will be shared.

Moreover, research can be done to assess how MSs and RPs can agree on a common standard for translating and formatting data which is shared to uniquely identify a citizen. Moreover, more research can be done as to what minimum combination of attributes uniquely identifies a citizen in each MS, and what the success rate is of identity matching attempts are across MSs.

Another avenue for further research is how the Dutch Ministry of the Interior can transition from the current identity matching process towards a different process, and what the implementation efforts and costs are for each solution direction. This could help the Ministry of the Interior to make a well-thought through decision for a solution direction.

Lastly, an interesting topic for further research is taking the LoA and type of RPs as a divisor for designing solution directions. A government-centric approach might be desirable for an authentication on LoA high, but undesirable for all LoAs (since the government would be able to track citizens for multitude of RPs, instead of a selection of RPs which require a high LoA for the provision of their services).

Appendix A: Abbreviations and Definitions

Attestation: the verification of a party regarding an attribute of a citizen.

BRP: Basisregistratie Personen: Dutch national registry which contains natural persons which live or have lived in the Netherlands.

BSN: Burgerservicenummer: Dutch citizen number. Each citizen should only have one BSN. The BSN is unique and is intended to remain persistent, even after a citizen's passing.

Citizen: a natural person which is a citizen of at least one MS.

eID mean: a notified[2] authentication mechanism of a MS. For the Netherlands, the notified eID mean for citizens is DigiD.

eIDAS Node: an interface of a MS used to communicate with other MSs' eIDAS nodes to identify a citizen in eIDAS 1.0.

eIDAS 1.0: Regulation (EU) No 910/2014 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.

eIDAS 2.0: A proposal to amend eIDAS 1.0. It introduces the concept of an EUDI-Wallet*.

EUDI-Wallet: A digital identity wallet with which citizens should be able to identify themselves digitally at every European public and large private organizations. The wallet also offers the possibility for citizens to share QEAA*.

---

[2] List of notified eID means: https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+available+attributes+of+pre-notified+and+notified+eID+schemes

Onboarding: a natural person with no pre-existing account at a RP seeks authentication at this RP.

First match: a natural person who has a pre-existing account at a RP seeks authentication with an EUDI-Wallet, of which the identification number used in the authentication procedure is not known to the RP.

Identity Provider: a party who stores and verifies information about natural persons (e.g. a government).

Member State (MS): a country which has signed the founding treaties of the European Union.

Polymorphic pseudonym: the result of an encryption of an identifier. One identifier can have multiple (i.e. polymorphic) pseudonyms which are derived from it.[3]

Relying Party (RP): A party where a citizen can request access to public or private services. A RP relies on the attributes of a citizen for identification purposes.

SPOF: Single Point of Failure.

Subsequent match: a natural person who has a pre-existing account at a RP seeks authentication with an EUDI-Wallet, of which the identification number used in the authentication procedure is known by the RP.

Unique identification: a process where person identification data or person identification means are matched with or linked to an existing account belonging to the same person. (Art. 3 (55) eIDAS).

[3] https://afsprakenstelsel.etoegang.nl/display/as/Polymorfe+pseudonimisering

Appendix B: Literature Review Article Inclusion

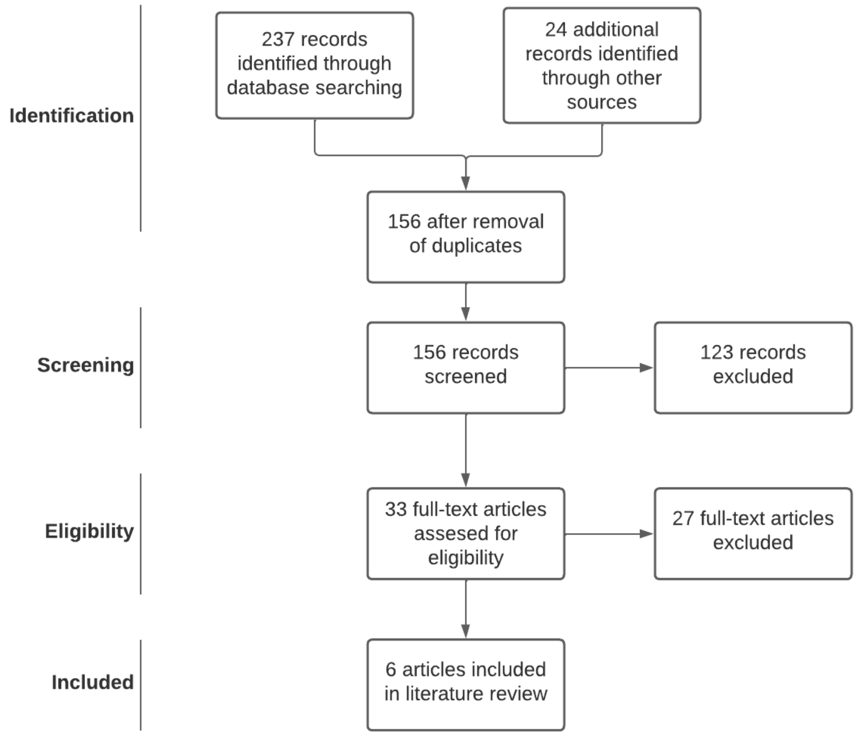

Figure 22: Article selection flow for articles on identity matching (based on the PRISMA method)

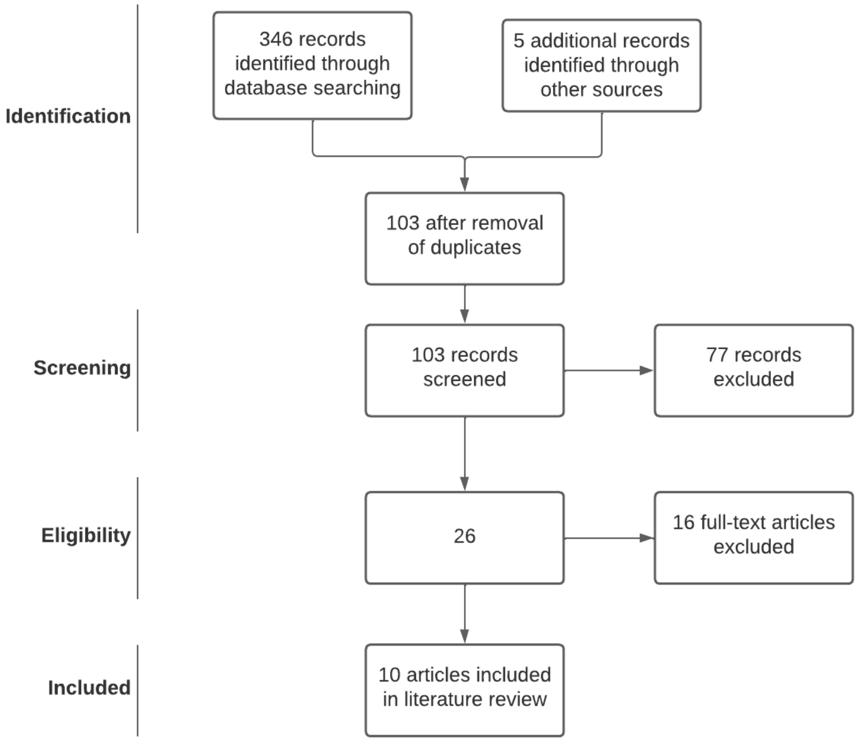

Figure 23: Article selection flow for papers on identity management (based on the PRISMA method)

The number of hits per search result on identity management is based on the results from 2004 onwards up until 09/11/2022.

Table 9: Search terms Scopus (to find theories on identity management)

Keywords	**Hits**	**Used**	**Duplicates**
“Identity Management”	3.919	4	N.A.
“Identity Management” AND Privacy	1.325	1	1
Federated OR Federation AND “Identity Management”	646	3	2
Federated OR Federation AND “Identity Management” AND Privacy	297	1	0
(User-centric OR User AND Centric) AND “Identity Management”	297	3	1
Identity AND Management AND eIDAS	38	1	0

The number of hits per search result on identity management is based on the results from 2014 onwards up until 09/11/2022.

Table 10: Search terms Scopus (to find problems on identity matching) (present in title, abstract, or key terms)

Keywords	**Hits**	**Used**	**Duplicates**
eIDAS	123	2	N.A.
Identity AND Matching AND (Europe OR EU OR European)	114	2	1
eIDAS AND Identity AND Matching	1	1	1
Once-only Principle AND Identity AND Matching	1	1	1

Table 11: Search terms Google (to find problems on identity matching)

Keywords	**Number of hits**	**Used**
eIDAS AND "Identity Matching" AND Barriers	182	1
“BSNk” AND Versleutelen AND Algoritme	9	2

Table 12: Articles and books included on identity management theories (section 4.3)

Articles Included	**Found through**
Benantar, M. (2005). *Access control systems: security, identity management and trust models*. Springer Science & Business Media.	(*Google Scholar*) Federated AND Identity AND Management
Jøsang, A., & Pope, S. (2005). User centric identity management. In *AusCERT Asia Pacific information technology security conference* (Vol. 22, p. 2005).	Referenced in Jøsang, AlZomai & Suriadi (2007)
Jøsang, A., AlZomai, M., & Suriadi, S. (2007). Usability and privacy in identity management architectures. In *ACSW Frontiers 2007: Proceedings of 5th Australasian Symposium on Grid Computing and e-Research, 5th Australasian Information Security Workshop (Privacy Enhancing Technologies), and Australasian Workshop on*	(*Scopus*) (User-centric OR User AND Centric) AND “Identity Management”

Health Knowledge Management and Discovery (pp. 143-152). Australian Computer Society.	
Chadwick, D. W. (2009). Federated identity management. In *Foundations of security analysis and design V* (pp. 96-120). Springer, Berlin, Heidelberg.	(*Scopus*) Federated AND Identity AND Management
Rieger, S. (2009, May). User-centric identity management in heterogeneous federations. In *2009 Fourth International Conference on Internet and Web Applications and Services* (pp. 527-532). IEEE.	(*Scopus*) (User-centric OR User AND Centric) AND "Identity Management"
Pfitzmann, A., & Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management.	(*Google Scholar*) Identity AND Management AND Terminology
Baldoni, R. (2012). Federated identity management systems in e-government: the case of Italy. *Electronic Government*, 9(1), 64-84.	(*Scopus*) Federated AND Identity AND Management
Slamanig, D., Stranacher, K., & Zwattendorfer, B. (2014, June). User-centric identity as a service-architecture for eIDs with selective attribute disclosure. In *Proceedings of the 19th ACM symposium on Access control models and technologies* (pp. 153-164).	(*Scopus*) (User-centric OR User AND Centric) AND "Identity Management"
Hörbe, R., & Hötzendorfer, W. (2015, May). Privacy by design in federated identity management. In *2015 IEEE Security and Privacy Workshops* (pp. 167-174). IEEE. Johannesson, P., & Perjons, E. (2014). *An introduction to design science* (Vol. 10, pp. 978-3). Cham: Springer.	(*Scopus*) Federated OR Federation AND "Identity Management" AND Privacy
Schwalm, S., Albrecht, D., & Alamillo, I. (2022). eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI. *Open Identity Summit 2022*.	(*Scopus*) "Identity AND Management AND eIDAS"

Table 13: Articles included on identity matching reliability problems (section 4.4)

Articles Included	**Found through**

Berbecaru, D. G., Lioy, A., & Cameroni, C. (2021). On Enabling Additional Natural Person and Domain-Specific Attributes in the eIDAS Network. *IEEE Access*, *9*, 134096-134121.	(*Scopus*) "eIDAS AND Identity AND Matching"
Krimmer, R., Dedovic, S., Schmidt, C., & Corici, A. A. (2021a, September). Developing cross-border e-Governance: Exploring interoperability and cross-border integration. In *International Conference on Electronic Participation* (pp. 107-124). Springer, Cham.	(*Scopus*) eIDAS
Krimmer, R., Prentza, A., Mamrot, S., Schmidt, C., & Cepilovs, A. (2021b). The Future of the Once-Only Principle in Europe. In *The Once-Only Principle* (pp. 225-236). Springer, Cham.	In the same journal as Leosk et al. (2021)
Leosk, N., Põder, I., Schmidt, C., Kalvet, T., & Krimmer, R. (2021). Drivers for and Barriers to the Cross-border Implementation of the Once-Only Principle. In *The Once-Only Principle* (pp. 38-60). Springer, Cham.	(*Scopus*) "Identity AND Matching AND Europe OR EU OR European"
Schmidt, C., Krimmer, R., & J Lampoltshammer, T. (2021). "When need becomes necessity"-The Single Digital Gateway Regulation and the Once-Only Principle from a European Point of View. *Open Identity Summit 2021*.	(*Scopus*) Cited in Krimmer et al. (2021b)
Schmidt, C., & Krimmer, R. (2022). How to implement the European digital single market: identifying the catalyst for digital transformation. *Journal of European Integration*, *44*(1), 59-80.	(*Scopus*) Referenced (Schmidt et al. 2021)

Table 14: Reports included in literature review

Reports Included	**Found Through**
Nora. (2017, April). *Startarchitectuur: Nationale implementatie van eIDAS met het stelsel Elektronische Toegangsdiensten*.	(Google) "BSNk" AND Versleutelen AND Algoritme

Verheul, E. R. (2019). *The polymorphic eID scheme*. Technical report, Ministry of Interior and Kingdom Relations The Hague The Netherlands.	(Google Scholar) Polymorphic AND Pseudonym AND eIDAS
Eurosmart. (2020, September). *Implementation of the eIDAS nodes: State of play*.	(Google) eIDAS AND Identity AND Matching
Hinsberg, H., Kala, K., Kask, L., & Kutt Anders (2020). *Study on Nordic-Baltic Trust Services.*	(Google) eIDAS AND "Identity Matching" AND Barriers

Appendix C: Requirements Interview Summaries

Interview 1

Goal:

The goal of the interviews was to understand the participant's view on the problem, as well as to elicit as many requirements as possible for the solution to the identity matching problems.

Method:

a semi-structured interview.

Participant:

Interviewee 1 (A-SIT Secure Information Technology Center)

Summary:

After an introduction from both sides, Herbert explained the context and workings of Identity Matching in Austria:

- Austria has experience with eIDs since the early 2000s
- Besides their population register, Austria has a supplementary register where non-Austrian citizens are registered who seek access certain services in Austria (such as non-Austrian citizens who temporarily work in Austria).

Regarding the identity matching process:

- When a person who is already enrolled in the supplementary register seeks to access an Austrian service with a new eID (= a different (e)ID which was used during the first authentication), the new eID is linked to the record of the person in the supplementary register. Therefore, the next time a person logs in with the same eID, Austria knows it pertains to the correct person.
- In the case mentioned above, identities need to be matched. Errors can occur here (e.g. through differences in formats between Austrian and foreign registers).
- Errors can also occur in national use cases: population registers stem from manual processes dating back to the early 2000s. Therefore, discrepancies within registers in

Austria can exist (e.g. someone is enrolled twice in the register, or two persons are listed as one person, called split and kitt cases respectively (“kitt” is German for “lute”)), although very rare.

- When an automated match cannot be established due to the abovementioned reasons, and the person which seeks to access the service complains about not getting access to their records or getting access to the wrong records (although the latter is unlikely, given that the algorithms aim at a safe default that biases to false negatives on matching rather than a false positive), a manual matching process is initiated. In this process, the person must provide additional evidence to prove that they are who they claim to be. These cases are rare.
- German citizens who cannot be matched due to multiple records in the supplementary register matches their name and date of birth (e.g. Hans Muller), and there is no common identifier linking the incoming citizen with the record, the German is asked for other data like e.g. the second residence address they have in Austria.

Regarding fraud:

- Herbert does not necessarily see realistic threats to someone applying for social benefits twice with an eID, since this system contains more safeguards than solely relying on the identity matching conversation at hand (e.g. you must have worked in Austria as well).
  - Only works if you manage to commit identity fraud twice while working in Austria and be those same two people you impersonate with an eID.
  - The digital system using eIDs does not make the process any more susceptive to fraud.
  - The digital system relies on the physical system of registries, which in turn relies on manual input. The problems resulting of this cannot be solved digitally.

Regarding a solution:

- Preferably re-use as much of the central identity matching infrastructure, which is currently in place, because:
  - Considerable investments have been made in the infrastructure, and
  - RPs do not want to match identities themselves.

- More and better information is needed to know what attributes uniquely identify an entity in each Member State (MS).
    - The peer review contains a large list of potential identity attributes.
    - It is not known which identity
    - Which attributes are generally available?
    - Which attributes are available at which identity provider?
    - Good example: Germany: published that they guarantee uniqueness with name at birth, date of birth and place of birth.
- Using the same set of attributes across Europe might be unrealistic, because it can differ per country which attributes guarantee uniqueness.
- MSs need to be able to rely on other MSs that when a persons' identifier expires, they do not reassign that identifier to another individual.

Requirements:

- An error rate is accepted for matches which are carried out automatically, since the party matching data simply never knows if the data on which the match is carried out is correct.
    - Even the date of birth of registered persons might change since there are refugees from which you simply do not know the birth date.
- MSs need to be able to rely on other MSs that when a citizen's identifier expires, they do not reassign that identifier to another individual.
- Preferably re-use as much of the central identity matching infrastructure which is currently in place.
- MSs must know from each other what attributes uniquely identify a citizen.
- MSs must know which standard attributes are available of citizens of other MSs, and which additional attributes are available in case a match cannot be established on the first instance.
- MSs must agree on data standards and formats of attributes shared.

Interview 2

Goal:

The goal of the interviews was to understand the participant's view on the problem, as well as to elicit as many requirements as possible for the solution to the identity matching problems.

Method:
a semi-structured interview.

Participant:
Interviewee 2 (Belastingdienst, i.e. Dutch Tax Office)

Summary:

After an introduction from both sides, Marco explains how citizens are uniquely identified at the Dutch tax office:

- At any identification request, the Belastingdienst always receives a name + BSN. They do not see whether a citizen is accessing the service through a Dutch or foreign eID mean.
  - Because the match is always executed on one number, the matching process is quite trivial.
- Mistakes have been made in the registration of natural persons in the Netherlands. This is due to the fact that the Netherlands went from multiple locally stored identifiers to one central registry (BRP) with one identifier (BSN). Errors include people with two BSNs, or a BSN which referred to the wrong citizen.
  - The Tax office normally finds out about these cases because an incident occurs and the individual in question reports it.
- Marco thinks there are citizens who pretend to be someone they are not to evade taxes.
  - A common case is a deceased citizen who lived abroad, of which the relatives remain receiving benefits.

In a hypothetical situation where there is no central identity matching infrastructure, and the citizen communicates directly with the RP:

- Since the Belastingdienst requires a BSN of the citizen, an EUDI-Wallet will always be required to send a BSN, either encrypted (PP-BSN) or not.

- Marco does not feel that RPs should be more involved in the decision making process on different identity matching solutions.

- The Netherlands has a well-kept national registry (BRP) and overall good internet access. It is therefore not necessary that information is stored on a citizen's device.

Requirements:

- The Belasting needs to receive an (encrypted) version of the BSN at an identification request.
- In case of no BSN, the citizen should be able to send additional attributes to verify their identity.

Interview 3

Goal:
The goal of the interview was to understand the expert's vision on the problem and to elicit requirements which are necessary to solve the reliability and privacy problems.

Method:
a semi-structured interview.

Participant:
Interviewee 3 (Dutch National Office for Identity Data (RvIG))

Summary:
Background information on the BRP (Dutch national registry of natural persons) and identity matching:

- The GBA was the first central digital registry of natural persons. Firstly just for inhabitants, later also for non-residents (2014).
- First identifiers were only sectoral: for instance social-fiscal numbers could only be used for social benefits and tax services. The demand for a communication between sectors grew, and therefore the demand for an cross-sectoral identifier. This resulted in the BSN.
- Sinds 2014 begonnen met de actieve registratie van niet-ingezetenen.
- Identity matching problems started appearing within the BRP. An example:
    - A Dutch citizen emigrates. This changes their status from inhabitant to non-inhabitant. After 15 years abroad and a new name due to a marriage, the citizen returns and is not matched to the BRP.
    - Solutions for this are that municipal officials can run queries in the BRP which seek to find a match with different percentages of certainty, and are instructed to ask for these kind of situations.
- Another problem situation encountered in the BRP now Is of incoming Ukrainian refugees' passports are written in Cyrillic, which is a different script than in which the Dutch language is written (Latin). When a Ukrainian citizen comes to the Netherlands, he or she is enrolled in the BRP with a translation of their name. Banks however note the Machine-Readable Zone (MRZ) which is noted on the passport. Since the translation and the MRZ tend not to match, refugees have difficulties with opening a bank account, since the Bank cannot find them in the BRP (which is required for opening a bank account).
- Ministry of the interior is responsible for the Dutch implementation of the eIDAS regulation relating to unique identification of foreign eIDs.

Functionalities of the central identity matching system at the eIDAS, BSN, and BRP Connector in the Netherlands:

- A score is given to a match based on the probability it is correct.
- The matchings algorithm takes common mistakes and translations of names into account (spelling such as 'sch' and 'tsch' is considered to match)
- Other MSs are positively intrigued by the matching process in the Netherlands.
- The benefits of the central matching process are:

- BRP is a very large dataset, easier to find a match than at RP level.
    - Causes RPs to have more assurance regarding the identity of a citizen.
  - Bundles knowledge on past matching anomalies.
- A BSN is not required at each identification: for instance, the judicial system does not care who pays a traffic ticket, as long as it is paid.
- Polymorphic pseudonyms allow for the BSN being communicated without passing it through in plain text to a RP.
- Even international standards on how data is noted contains ambiguity: the ICAO standard offers three possible ways to note a 'ü' from the MRZ: ue, ux, of u.
- The eIDAS Minimum Data Set (MDS) is too limited to ensure unique identification. The data sets used for unique identification are more encompassing on an international level (for instance in the domain of international social security), since there is more experience with uniquely identifying citizens. They take the birth dates of parents into account, which is a good knockout criterium.
- The BRP is getting an update where it is possible for government officials to search for matches, but without getting access to all data of a citizen, to improve the privacy of citizens.

Data on % of correct matches:

- From a sample of 120 identity matching attempts of a foreign eID mean at the BRP Connector, 84 attempts (70%) lead to a correct match, 19 attempts (15.8%) do not match any record, and 17 attempts (14.2%) lead to one or more matches, but these do not correspond to the citizen identifying themselves

Regarding fraud:

- Believes there are risks for fraud using eID means/EUDI-Wallets.
- Risk of false negatives is greater than the risk of false positives, since it is very easy to have a false negative due to issues in data entries, translation of data etc. The chance of there being an error in your data which makes all your records 100% correspond with those of another citizen is smaller.

Requirements for a solution:

- Expanding the eIDAS MDS with additional attributes

- Agreements between MSs between data formats, notation, and translation
- More knowledge regarding matching processes and problems of other MSs
    - Maybe bundle this knowledge in 1 API.
- More knowledge necessary regarding which combination of attributes uniquely identify a citizen in other MSs.
- Names are subject to too much change for the purpose of identity matching:
    - Seek matches based on other attributes.
    - For instance only the date of birth of the citizen and the citizen’s mother.
- After the first identification request of a foreign citizen in the Netherlands, the eIDAS connector could be obsolete for subsequent identification requests.

Appendix D: Extent to which Requirements are Fulfilled

Table 15: Extent to which reliability requirements are fulfilled

#	Central	Hybrid	Wallet provider-centric
RR1	After the first identification request, the RP receives the same identifier. For subsequent identifications, a RP only needs one number to match their database, because the identifier is unique, persistent, and only related to one citizen. The requirement is therefore **met**.	After the first identification request, the RP receives the same identifier. For subsequent identifications, a RP only needs one number to match their database, because the identifier is unique, persistent, and only related to one citizen. The requirement is therefore **met**.	After the first identification request, the RP receives the same identifier. For subsequent identifications, a RP only needs one number to match their database, because the identifier is unique, persistent, and only related to one citizen. The requirement is therefore **met**.
RR2	At the first identification attempt of a citizen with a foreign EUDI-Wallet at a Dutch RP which is allowed to process the BSN, the citizen is uniquely identified in the BRP using the citizen's PID, and the citizens BSN (if they provide this). Due to the constraints regarding agreements on the content and format of PID data, the citizen should be uniquely identifiable within the BRP. The requirement is therefore **met.**	**Met.** For the same reason as with the central approach.	**Met.** For the same reason as with the central approach.
RR3	The identifier received by the citizen is accompanied by a digital signature by the BSN Connector which proves the authenticity and integrity of the identifier. By comparing the certificate	**Met.** For the same reason as with the central approach.	The HSM creates the identifiers only after the citizen is successfully onboarded, and therefore has been identified by the BSN Connector. The HSM

	with the identifier which the RP receives of the citizen, the RP can check its authenticity and integrity. The requirement is therefore **met**.		contains logic which only permits identifiers to be constructed as the Dutch government intends. Moreover, the identifiers created also carry a digital signature of the BSN Connector. The requirement is therefore **met**.
RR4	**Met.** For the same reason as under RR3.	**Met.** For the same reason as under RR3.	**Met.** For the same reason as under RR3.
RR5	When a citizen seeks identification with a new EUDI-Wallet, while this citizen has previously onboarded another EUDI-Wallet, there are two optional flows: one where the incoming eIDAS identifier is the same as with the previously onboarded EUDI-Wallet, and one where the eIDAS identifier is the same. When the identifiers are different, the user's PID needs to be matched to the Dutch national registry. When the correct match is found, the new EUDI-Wallet will be given the same eIDAS identifier as the first wallet, new EUDI-Wallet ID is saved at the eIDAS Connector. The citizen does not need to be found in the national registry, since the eIDAS identifier is present in the mapping table of the eIDAS Connector. Therefore, the requirement is **met.**	**Met.** For the same reason as with the central approach.	**Met.** For the same reason as with the central approach.
RR6	The BSN and eIDAS Connector are needed for each identification request of	The BSN and eIDAS Connector are only needed	The Dutch government does not have access to any identification

	a citizen. Therefore, the requirement is **not met.**	for each first identification request of a citizen at a RP. Subsequent identification requests do not require an intervention by the BSN and eIDAS Connector. Therefore, the requirement is **not met.**	request of a citizen since the BSN and eIDAS connector only serve to supply the HSM with the correct key pairs. Where the keys are used is not accessible for the BSN and eIDAS Connector. The requirement is therefore **met.**

Table 16: Extent to which privacy requirements are fulfilled

#	Central	Hybrid	Wallet provider-centric
PR1	The PID is only sent to the eIDAS Connector the first identification request, whilst for subsequent identifications solely the eIDAS identifier is used. Therefore, subsequent identifications minimize the use of personal data. Regarding the supervision of what personal data is relevant: access rights are controlled by the Dutch Ministry of the Interior and the Dutch Ministry of Economic Affairs for every identification request. Regarding the storage of personal information: only the eIDAS identifier and the identifier which is used for the identification request are stored in the eIDAS Connector. This is all which is necessary in the current architecture to fulfill the purpose of unique identification. The hybrid and wallet provider-centric solution directions however store less information about citizens for the same purpose. Therefore, this requirement is **not met.**	A citizen only sends their PID for new identification requests, and therefore only sends what is necessary to ensure unique identification (assuming that the access rights of a RP have been determined correctly). Regarding the supervision of what personal data is relevant: access rights are controlled by the citizen's wallet for every identification request. Regarding the storage of personal information: only the eIDAS identifier and the identifier which is used for the identification request are stored in the eIDAS Connector. This is all which is necessary in the current architecture to fulfill the purpose of unique identification. If unique identification is not necessary (only an attestation of a valid wallet), nothing is stored in the eIDAS Connector (because the citizen sends the credential directly to the RP). The requirement is **met.**	A citizen only sends their PID if a BSN is required for the requested service, and the citizen does not have an encrypted BSN in their wallet. Therefore, the citizen only needs to load the encrypted BSN once in their wallet, and the PID is not stored in the eIDAS Connector. Regarding the supervision of what personal data is relevant: access rights are controlled by the citizen's wallet for every identification request. Regarding the storage of personal information: only the eIDAS identifier and an encrypted BSN are stored in the eIDAS Connector. All other identifiers are stored on the citizen's wallet. This is all which is necessary in the current architecture to fulfill the purpose of unique identification. The requirement is **met.**

PR2	Yes, access rights are controlled by the Dutch Ministry of the Interior and the Dutch Ministry of Economic Affairs for every identification request. The requirement is **met.**	The access rights of a RP are reviewed by a citizen's wallet. This is a different approach than is currently in place. The way in which RPs and their access rights will be registered is still a topic of debate (WG3, 2022). The requirement is **met.**	The access rights of a RP are reviewed by a citizen's wallet. This is a different approach than is currently in place. The way in which RPs and their access rights will be registered is still a topic of debate (WG3, 2022). Therefore, it is not yet known whether this way of assessing access rights will meet this requirement. The requirement is **met.**
PR3	There are two key pairs which encrypt the citizen's identifiers. One is for encrypting the BSN, and the other is for encrypting the eIDAS identifier. Since the keys are different, the outcome of the encryption is different, and therefore no one can assess whether an encrypted BSN and eIDAS identifier correspond to the same citizen. Therefore, the requirement is **met.**	**Met.** For the same reason as with the central approach.	**Met.** For the same reason as with the central approach.
PR4	The BSN is never shared in plaintext outside of the BSN and eIDAS Connector. Moreover, when the encrypted format is shared, this is never decryptable by the EUDI-Wallet provider. Therefore, this requirement is **met.**	**Met.** For the same reason as with the central approach.	The BSN is never available outside of the HSM in plain text. Even though the HSM is stored at the EUDI-Wallet provider, it does not have access to its content. Therefore, the requirement is **met.**
PR5	**Met.** The identifier a citizen uses is never sent to the EUDI-Wallet	**Met.** For the same reason as with the central approach.	The RP specific identifier is not visible to the EUDI-Wallet

	provider, but directly to the EUDI-Wallet.		provider because it is ‘re-keyed’ and ‘re-shuffled’ upon sending, as described by Verheul (2019). Therefore, the EUDI-Wallet provider does not have access to the BSN of a citizen. Therefore, the requirement is **met.**
PR6	Because the identifier which is sent to the RP is encrypted using the public key of that RP, only the RP which is intended to see the identifier can have access to it and is therefore the only entity which can assess to which citizen it corresponds. The requirement is therefore **met**.	**Met.** For the same reason as with the central approach.	**Met.** For the same reason as with the central approach.
PR7	The encrypted identifiers which are intended not to be decryptable are an encrypted version of the hash value of that identifier. Since the hash value does not correspond to the content of this identifier, no RP can cryptographically derive the underlying identifier. The requirement is therefore **met**.	**Met.** For the same reason as with the central approach.	**Met.** For the same reason as with the central approach.
PR8	The BSN and eIDAS Connector have access to each identification request of a citizen. Therefore, the requirement is **not met.**	The BSN and eIDAS Connector have access to each first identification request of a citizen at a RP. Subsequent identification requests are not accessible for the BSN and eIDAS Connector. Therefore, the requirement is **not met.**	The BSN and eIDAS Connector have access to each identification request of a citizen since the BSN and eIDAS connector only serve to supply the HSM with the correct key pairs. Where the keys are used is not accessible for the BSN and

			eIDAS Connector. The requirement is therefore **met.**

Appendix E: Morphological Charts

Table 17: Government-centric approach mapped to morphological chart

#	Function	Mean 1	Mean 2	Mean 3	Mean 4
1	Where are identifiers created	Dutch Government	EUDI-Wallet	EUDI-Wallet Provider	
2	Where previous are identifiers stored	Dutch Government	EUDI-Wallet	EUDI-Wallet Provider	Identifiers are deleted after unique identificaiton has been established
3	Who checks access rights of a RP	Dutch Government	EUDI-Wallet	EUDI-Wallet Provider	Access rights are not checked.
4	Who can access first identification attempts	Dutch Government	EUDI-Wallet	EUDI-Wallet Provider	
5	Who can access subsequent identification attempts	Dutch Government	EUDI-Wallet	EUDI-Wallet Provider	
6	Who can access identifiers of citizens used at RPs	Dutch Government	EUDI-Wallet	EUDI-Wallet Provider	

Table 18: Hybrid approach mapped to morphological chart

#	Function	Mean 1	Mean 2	Mean 3	Mean 4
1	Where are identifiers created	Dutch Government	EUDI-Wallet	EUDI-Wallet Provider	
2	Where previous are identifiers stored	Dutch Government	EUDI-Wallet	EUDI-Wallet Provider	Identifiers are deleted after unique

					identificaiton has been established
3	Who checks access rights of a RP	Dutch Government	EUDI-Wallet	EUDI-Wallet Provider	Access rights are not checked.
4	Who can access first identification attempts	Dutch Government	EUDI-Wallet	EUDI-Wallet Provider	
5	Who can access subsequent identification attempts	Dutch Government	EUDI-Wallet	EUDI-Wallet Provider	
6	Who can access identifiers of citizens used at RPs	Dutch Government	EUDI-Wallet	EUDI-Wallet Provider	

Table 19: Wallet provider-centric approach mapped to morphological chart

#	Function	Mean 1	Mean 2	Mean 3	Mean 4
1	Where are identifiers created	Dutch Government	EUDI-Wallet	EUDI-Wallet Provider	
2	Where previous are identifiers stored	Dutch Government	EUDI-Wallet	EUDI-Wallet Provider	Identifiers are deleted after unique identificaiton has been established
3	Who checks access rights of a RP	Dutch Government	EUDI-Wallet	EUDI-Wallet Provider	Access rights are not checked.
4	Who can access first identification attempts	Dutch Government	EUDI-Wallet	EUDI-Wallet Provider	
5	Who can access subsequent identification attempts	Dutch Government	EUDI-Wallet	EUDI-Wallet Provider	

6	Who can access identifiers of citizens used at RPs	Dutch Government	EUDI-Wallet	EUDI-Wallet Provider	

Appendix F: Evaluation Miro-board input

Table 20: From participant input to TOE variables (Central approach, 1st focus group)[4]

	Input of participants	**Abstraction**
Benefits	unified & centralized approach	Centralization
	standardized processes	Standardization
	reuse of existing infrastructure	Reuse of infrastructure
	leverage existing RP registrations	Reuse of (back office) data
	leverage existing matches (to the extent this is possible)	Reuse of (back office) data
	user friendly: 1 time RM instead of a hassle: every time the user logs on RM	User-friendliness
Barriers	Single Point of Failure (SPOF) and high dependence	SPOF
Points to consider	attestation of RM outcome will improve user experience (compared to RM every time a user logs on, which will increase the administrative burden)	Attestations instead of consecutive matches
	cost sharing for the collective boundary resource	Cost model of boundary resource
	Feasibility and attractiveness of central approach depends on the cost of changing existing infrastructure, reuse of eIDAS 1 identifiers.	Reuse of infrastructure
	potential extra steps in user flow necessary	User-unfriendliness

[4] There was no time for the evaluation of the wallet provider-centric approach in the first focus group session, and therefore it has only been evaluated in the second focus group.

Table 21: From participant input to TOE variables (Hybrid approach, 1st focus group)

	Input of participants	Abstraction
Benefits	might be useful for most MSs since it reuses existing matches and infrastructure	Reuse of infrastructure
	allows tailored solutions	Allows modularity
	Should eliminate tracking of citizens	Tracking of citizens (positive)
Barriers	still privacy implications like linkability tracking and tracing by the government (IdP)	Tracking of citizens (negative)
	doubts about the feasibility of implementing one/different encryption scheme which is compatible with all 27 MSs	Cryptographic interoperability with other MSs (negative)
	requires changing IDM functionality to be independent of the eIDAS node authentication flow	SPOF
Points to consider	seems to need tailored logic in the wallet/possibly per MS	Additional logic requirements needed of wallet
	doubts whether it will lead to a user-friendly process	User friendliness (negative)

Table 22: From participant input to TOE variables (Central approach, 2nd focus group)

	Input of participants	**Abstraction**
Benefits	Maximum reuse of existing infrastructure	Reuse of infrastructure
	MSs do not have to support polymorphic identifiers	Cryptographic interoperability with other MSs (negative)
	PID provider can collect data for crime prevention	Reuse of (back office) data
Barriers	Makes wallet use dependent on online availability (cf offline use case and single point of failure)	Dependency on online availability
	Tracking can get an issue	Tracking of citizens (negative)
Points to consider	How are the messages send form the wallet to other parties? Through the eIDAS node? Or directly?	Reuse of infrastructure
	eIDAS currently has a privacy issue with the mapping table: they may only retain it for so long. We could place the proof of mapping in the Wallet, to avoid this issue.	Privacy hotspot at IdP

Table 23: From participant input to TOE variables (Hybrid approach, 2nd focus group)

	Input of participants	**Abstraction**
Benefits	Seems to also fit to existing eIDAS 1.0 infrastructures (like the central approach)	Reuse of infrastructure
	Avoids central authority tracking activity (but it still knows 'relations' between citizens and RPs (i.e. which RP a citizen has authenticated at))	Tracking of citizens (positive)
Barriers	Every MS has to implement this kind of identifiers (polymorphic identifier?) and migrate existing identifiers to polymorphic identifiers and in the worst case implement decryption module	Cryptographic interoperability with other MSs (negative)
	Central authority still knows 'relations' between citizens and RPs)	Tracking of citizens (negative)
	Makes wallet use dependent on online availability (cf offline use case and single point of failure)	Dependency on online availability
	Privacy implications like linkability, tracking and tracing by the government (IDP?) User can still be linked, since use of BSN by every RP.	Tracking of citizens (negative)
Points to consider	One option for provisioning could be to use notified eID mean to transport PID to the RP. This create a less user-friendly solution, since the user has to login with eID mean for every new encountered RP. This could be a practical implementation since the eID mean is mandatory to activate/enroll the wallet.	User friendliness (negative)

Table 24: From participant input to TOE variables (Wallet provider-centric approach, 2nd focus group)

	Input of participants	Abstraction
Benefits	Most privacy friendly version. The user has more control over own identifier.	Tracking of citizens (positive)
	Easiest to communicate to the public	Easy to communicate to the public
	Continuity and scalability.	Continuity and scalability
	Least dependent on central services	Least dependency on central services
Barriers	HSM provider still needs to know which RP is authenticated against. Perhaps it is possible to avoid this.	Tracking of citizens (negative)
	Huge investment for MSs RPs to communicate with the wallet	Large investments
	(complex?) logic in the wallet.	Additional logic requirements needed of wallet
Points to consider	HSM component is still a central party?	Centralization
	Why polymorphic pseudo? If the wallet generates it, wouldn't a simple pseudonym suffice?	Why Polymorphic Pseudonyms
	In case of a legitimate interest of the RP (e.g. litigation), can the PID issuer trace the pseudonym back to the natural person?	Legitimate tracking possible?
	Loss of wallet is loss of wallet-side mapping table?	Does loss of wallet mean loss of the mapping table?
	The user has more control over own identifier. Could be better if this identifier was generated in de wallet per MS or RP, since this would mitigate the risks of likability by RPs. But then again, this would not comply to the Regulation, which states usage of uniquely persistent	More control over identifier. Maybe create identifiers within wallet

	identifiers (UPI). I would recommend not to use UPI, because this enables likability.	

References

Authenticatiedienst als verwerker van het BSN. (2022, September 7). Afsprakentoestel Elektronische Toegangsdiensten. https://afsprakenstelsel.etoegang.nl/display/as/Authenticatiedienst+als+verwerker+van+het+BSN

Attewell, P. (1992). Technology diffusion and organizational learning: The case of business computing. *Organization science*, *3*(1), 1-19.

Baker, J. (2012). The technology–organization–environment framework. *Information systems theory*, 231-245.

Baldoni, R. (2012). Federated identity management systems in e-government: the case of Italy. *Electronic Government*, 9(1), 64-84.

Berbecaru, D. G., Lioy, A., & Cameroni, C. (2021). On Enabling Additional Natural Person and Domain-Specific Attributes in the eIDAS Network. *IEEE Access*, *9*, 134096-134121.

Bradford, M., Earp, J. B., & Grabski, S. (2014). Centralized end-to-end identity and access management and ERP systems: A multi-case analysis using the Technology Organization Environment framework. *International Journal of Accounting Information Systems*, *15*(2), 149-165.

CEF Digital. (2022, 28 February). *Overview of available attributes of pre-notified and notified eID schemes - eID User Community* -. Geraadpleegd op 10 april 2022, van https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+available+attributes+of+pre-notified+and+notified+eID+schemes

Commissiedebat Nr. 938, gehouden op 31 mei 2022, over Telecomraad (Formeel) d.d. 3 juni 2022.

Davis, F. D. (1986). A technology acceptance model for testing new end-user information systems: theory and results. *Sloan School of Management*, *291*.

Dougan, T., & Curran, K. (2012). Man in the browser attacks. *International Journal of Ambient Computing and Intelligence (IJACI)*, *4*(1), 29-39.

Dube, T., Van Eck, R., & Zuva, T. (2020). Review of technology adoption models and theories to measure readiness and acceptable use of technology in a business organization. *Journal of Information Technology*, *2*(04), 207-212.

Recker, J. (2008). BPMN modeling-who, where, how and why. *BPTrends*, 1-8.

Regulation (EU) No 910/2014 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.

Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014.

European Commission (2021). Proposal for amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.

Eurosmart. (2020, September). *Implementation of the eIDAS nodes: State of play*. https://www.eurosmart.com/wp-content/uploads/2020/09/Eurosmart_study_eIDAS_nodes_interconnection_final.pdf

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, 75-105.

Hörbe, R., & Hötzendorfer, W. (2015, May). Privacy by design in federated identity management. In *2015 IEEE Security and Privacy Workshops* (pp. 167-174). IEEE.

Johannesson, P., & Perjons, E. (2014). *An introduction to design science* (Vol. 10, pp. 978-3). Cham: Springer.

Kanne, P., & Löb, N. (2016, October). (Digitale) contacten met de overheid. In *Kennis Openbaar Bestuur*. Retrieved October 19, 2022, from https://kennisopenbaarbestuur.nl/media/254288/digitale-contacten-met-de-overheid.pdf

Krimmer, R., Dedovic, S., Schmidt, C., & Corici, A. A. (2021a, September). Developing cross-border e-Governance: Exploring interoperability and cross-border integration. In *International Conference on Electronic Participation* (pp. 107-124). Springer, Cham.

Krimmer, R., Prentza, A., Mamrot, S., Schmidt, C., & Cepilovs, A. (2021b). The Future of the Once-Only Principle in Europe. In *The Once-Only Principle* (pp. 225-236). Springer, Cham.

Leosk, N., Põder, I., Schmidt, C., Kalvet, T., & Krimmer, R. (2021). Drivers for and Barriers to the Cross-border Implementation of the Once-Only Principle. In *The Once-Only Principle* (pp. 38-60). Springer, Cham.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & Prisma Group. (2009). Reprint—preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Physical therapy*, *89*(9), 873-880.

Moniava, G., Verheul, E., & Schoenmakers, L. (2008). Extending DigiD to the private sector (DigiD-2). *Department of Mathematics and Computing Science, Eindhoven University of Technology*.

Nora. (2017, April). *Startarchitectuur: Nationale implementatie van eIDAS met het stelsel Elektronische Toegangsdiensten*. https://www.noraonline.nl/images/noraonline/5/57/Startarchitectuur_NL_implementatie_eIDAS_met_eTD_1_2.pdf

Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. *Electronic Journal of Information Systems Evaluation*, *14*(1), pp110-121.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, *24*(3), 45-77.

Pfitzmann, A., & Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management.

Rogers, E. (1995). Diffusion of Innovations (Fourth Paperback ed.).

Rieger, S. (2009, May). User-centric identity management in heterogeneous federations. In *2009 Fourth International Conference on Internet and Web Applications and Services* (pp. 527-532). IEEE.

Schmidt, C., & Krimmer, R. (2022). How to implement the European digital single market: identifying the catalyst for digital transformation. *Journal of European Integration*, *44*(1), 59-80.

Schmidt, C., Krimmer, R., & J Lampoltshammer, T. (2021). "When need becomes necessity"-The Single Digital Gateway Regulation and the Once-Only Principle from a European Point of View. *Open Identity Summit 2021*.

Slamanig, D., Stranacher, K., & Zwattendorfer, B. (2014, June). User-centric identity as a service-architecture for eIDs with selective attribute disclosure. In *Proceedings of the 19th ACM symposium on Access control models and technologies* (pp. 153-164).

Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). *Processes of technological innovation*. Lexington books.

Tsakalakis, N., Stalla-Bourdillon, S., & O'hara, K. (2018, August). Data protection by design for cross-border electronic identification: Does the eIDAS interoperability framework need to be modernised?. In *IFIP International Summer School on Privacy and Identity Management* (pp. 255-274). Springer, Cham.

Tweede Kamer, Parlementair onderzoek naar ICT-projecten bij de overheid, vergaderjaar 2014-2015, 33 326, nr. 5.

van Huffelen, A. (2022) Kamerbrief voortgang Europese Digitale Identiteit. https://www.rijksoverheid.nl/documenten/kamerstukken/2022/08/17/kamerbrief-voortgang-europese-digitale-identiteit

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*, 425-478.

Verheul, E. R. (2019). *The polymorphic eID scheme*. Technical report, Ministry of Interior and Kingdom Relations The Hague The Netherlands.

vom Brocke, J., & Maedche, A. (2019). The DSR grid: six core dimensions for effectively planning and communicating design science research projects. *Electronic Markets*, *29*(3), 379-385.

von der Leyen, U. (2020). *State of the Union Address*. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

VVD, D66, CDA & Christenunie. (2022*). Coalitieakkoord 2021 – 2025: Omzien naar elkaar, vooruitkijken naar de toekomst.*
https://www.rijksoverheid.nl/documenten/publicaties/2022/01/10/coalitieakkoord-omzien-naar-elkaar-vooruitkijken-naar-de-toekomst

Wang, H. J., & Lo, J. (2016). Adoption of open government data among government agencies. *Government Information Quarterly*, *33*(1), 80-88.

WG3 *Reliance on the Wallet* (2022) D.6 Cover Note Identification / Identity Matching, Draft Version 0.4.