University of Amsterdam

Research Project 2

Design Exploration of Transparency Enhancing Technology for Government

Author:
M. Houtenbos

Supervisor:
Dr. G. van 't Noordende

A research project report submitted in fulfillment of the requirements for the degree of Master of Science

in the

Master System and Network Engineering
Graduate School of Informatics (GSI)

February 11, 2016

University of Amsterdam

“*The very word "secrecy" is repugnant in a free and open society; and we are as a people inherently and historically opposed to secret societies, to secret oaths and secret proceedings. We decided long ago that the dangers of excessive and unwarranted concealment of pertinent facts far outweighed the dangers which are cited to justify it. Even today, there is little value in opposing the threat of a closed society by imitating its arbitrary restrictions. Even today, there is little value in insuring the survival of our nation if our traditions do not survive with it. And there is very grave danger that an announced need for increased security will be seized upon those anxious to expand its meaning to the very limits of official censorship and concealment. That I do not intend to permit to the extent that it is in my control. And no official of my Administration, whether his rank is high or low, civilian or military, should interpret my words here tonight as an excuse to censor the news, to stifle dissent, to cover up our mistakes or to withhold from the press and the public the facts they deserve to know.*”

– J.F. Kennedy

“*Civilization is the progress toward a society of privacy. The savage’s whole existence is public, ruled by the laws of his tribe. Civilization is the process of setting man free from men.*”

– Ayn Rand

UNIVERSITY OF AMSTERDAM

Abstract

Faculty of Science (FNWI)
Graduate School of Informatics (GSI)

Master of Science

Design Exploration of Transparency Enhancing Technology for Government

by M. Houtenbos

This research project involves a design exploration of transparency enhancing technology that can be used by the Dutch government to provide transparency of the data stored on citizens. We will attempt to outline a potential solution that does not negatively impact citizen privacy when aggregating personal data from many different government agencies and local governments. Existing technical solutions do not provide the transparency, privacy, and security required to promote strong trust and confidence in such a system. Our proposed design provides a theoretical basis for a system that satisfies the government requirements and provides privacy and security by design. The research performed for this project consists of a study of related research, standards, and existing technology, as well as exploring the social roles of technology in our society, and finally testing the technical feasibility of our proposed design. With this design exploration we believe we have shown that it is feasible to design a transparency enhancing system for use by the government without negatively impacting citizen privacy.

Acknowledgements

I would like to express my very great appreciation to Dr. G.J. (Guido) van 't Noordende for his valuable and constructive feedback during this research project. Especially his focus on a top down approach helped me out tremendously. His willingness to make time in his busy schedule to offer me guidance is very much appreciated.

I would also like to offer my special thanks to my teacher Dr. C.J.P. (Karst) Koymans for his technical feedback and suggestions. I am very happy to have a teacher that can provide both his extensive technical expertise as well as enthusiastic personal encouragement.

Furthermore I would like to thank Drs. Ing. N.P.H. (Niels) Sijm, Mr. T. (Tom) Demeyer, and Mr. H. (Hans) de Zwart for taking the time to sit down and talk about this subject. Their useful contributions and personal recommendations really helped shape the direction of the research project.

Finally I wish to acknowledge the support of my family, who stood by my side and helped me navigate new uncharted territories of stress levels.

Contents

Chapter 1

Introduction

1.1 Introduction

For this research project we will perform a design exploration of transparency enhancing technology for government, which consists of comparing advantages and disadvantages of a couple different levels of distribution and encryption key management systems that balances transparency with privacy and security.

The (theoretical) technical solutions suggested in this report should outline practical solutions to the Dutch government aim to allow citizens easy online access to all their digital data as described amongst others in *"Visiebrief Digitale Overheid 2017"*[1] and *"Overheidsbrede Dienstverlening 2020"*[2] (see appendix A for list of participating government agencies). Both the target for 2017 and 2020 are logical continuations of the *"Digitale Agenda.nl"* [3][4], and the *"Uitvoeringsprogramma Dienstverlening En E-Overheid"* which concluded in 2014 [5][6][7]. The temporal context of these documents is outlined in the timeline summary in appendix B.

In practice these goals are being worked out by the Manifestgroep[1] (a coalition of different government branches founded in 2003), the Forum Standardization[2] (which was established in 2006, and tasked with writing expert recommendation on the use of open standards and technology) [8]. Implementations of government systems are currently being developed and maintained by Logius[3] (the official digital government service established in 2006 as GBO[4]) [9]. The current government reaffirmed these course in their coalition agreement and further actions [10].

In the *"Manifestgroep Workbook"*[11] good service for the citizen comes first (requiring linking of government's systems). Additionally, the government should show the citizen what data they store, and the citizen has to give permission before the data can be used. Read and write access are needed, allowing the citizen to read data from multiple government organizations, and write data that can be used by multiple organizations in one place. This is exemplified in the following quote:

[1] https://manifestgroep.pleio.nl/manifestgroep

[2] https://www.forumstandaardisatie.nl/english/

[3] https://www.logius.nl/

[4] https://www.logius.nl/over-logius/jaaroverzichten/jaaroverzicht-2009/over-logius/

> *"Als klant hoef ik gegevens maar één keer aan te leveren en kan ik gebruik maken van proactieve diensten. Der [sic] overheidsorganisaties maken inzichtelijk wat zij van mij weten en gebruiken mijn gegevens niet zonder mijn toestemming."*[11]

The proper balance between privacy and transparency of all data the government gathers about citizens is still a sociologically, procedurally and technologically unresolved question towards which this research project aims to contribute a part of a solution.

1.2 Motivation

"Transparency" can have different meaning depending on context. In this case, transparency refers to the transparency of the government, and specifically the data that is stored about its citizens. The motivation for this research project lies in the Dutch government's plans to use technology to increase transparency about which data is stored by all government agencies - including local government and semi-government - and the recognition of the inherent risks of technology that unifies access to data from multiple government agencies to increase transparency towards citizens.

Government databases generally contain a lot of privacy sensitive data on citizens. In the wake of a large database leak in the UK, a report was commissioned that evaluated the privacy risks of all existing government databases. The researchers found that of the 46 databases they analyzed 40 had privacy issues, 11 of which almost certainly had human rights or data protection violations. A cause of this huge collection of privacy violating databases was found in the government's ambition to build online centralized databases to facilitate the sharing of data across different agencies, while promising the public more choice and personalization in their interaction with government [12]. The contemporary Dutch government plans and promises ring a decade old familiar bell. One crucial difference from the old UK database state is that the Dutch ambition is to make all these databases with citizen data available trough one system. Large aggregate databases are an even more valuable target and pose a higher risk to privacy because a lot more can be inferred from aggregate data than disjoined data sets. To mitigate these risks, access to the system must be carefully controlled [13]. Transparency and privacy may thus seem diametrically opposed, however we set out to prove this is not necessarily the case.

Our motivation to find a middle ground stems from the immeasurable value that transparency, privacy, and security hold for a functioning democracy. The government goals to provide more transparency, privacy, and security, as well as convenience makes this an opportune moment to perform research into technology that can contribute to bringing balance to these values. We are thus motivated to attempt to construct a design that satisfies these requirements.

Creating a design that offers transparency without sacrificing privacy is a complex subject that requires sociological, procedural and technical problems to be solved. While there will certainly be a strong focus on technical security of the design, the procedural plan will determine the real transparency and privacy offered by the design in a real world scenario. Both the procedural and technical design must have a strong basis to have a good system design. Finally the sociological plan will likely be of equal importance to allow the design to be successful in practice, since a system that does (somewhat) conform to familiar social experiences has a higher chance of being appropriated by people. It is thus advisable to take a pragmatic approach to designing the social aspects of this system [14].

1.3 Focus of Research

1.3.1 Research Question

The research question on which is focused is stated as:

> *" **How could transparency enhancing technology be designed for use by the government without negatively impacting citizen privacy?** "*

To be able to answer this abstract research question we look at the practical case of a system envisioned by the Dutch government.

1.3.2 Requirements

The following requirements are based on various documents released by the Dutch government. Some of these requirement are based on citizen rights and/or government duties already written in law, others are in the process of being written in law, and some are stated as future goals. A more thorough summary of our interpretation of the stated requirements and references to their sources is listed in appendix C.

1. ***Users (citizens) have a right to know what data is stored by various (government) agencies***
2. ***Users should only have to provide their data to the government in one place***
3. ***A system to which both users and agencies connect is needed to facilitate this***
4. ***Users must be able to authenticate securely with a strong personal identification mechanism***
5. ***Multiple strong authentication mechanisms must be supported, specifically international alternatives***
6. ***Agencies can securely and verifiably enter, modify and read (a subset of) data stored on a user***
7. ***Users can view their data stored by agencies and enter and modify their own personal data***
8. ***Users can give permissions to other users and agencies to access (a subset of) their data***

9. ***Users can issue a mandate to another user to allow this user to manage their data***
10. ***Agencies can issue a mandate to other agencies/users (employees) to access data of users (citizens)***
11. ***Users can revoke permissions, including default permissions to agencies***
12. ***It must be possible to verify system functionality, providing a transparent transparency system***
13. ***Data stored in the system must only be accessible to users and agencies that are authorized***
14. ***Agencies can read and write data to each user within the agency namespace by default***
15. ***An agency can request a user to allow access to personal data or data written by another agency***
16. ***Users can to issue temporary permissions to other users or agencies***
17. ***Additional keys can be created that are authenticated descendants or alternatives to the first government-issued ID***
18. ***Users can be identified with multiple persistent pseudonyms instead of only their BSN***

1.4 Methodology

1.4.1 Procedure

To perform our design exploration of transparency enhancing technology for use by government we shall start by summarizing related work. We will look at the relation between transparency, security, and privacy. How these three sociological aspects may be of importance to the success of such a system will be explored. Related technological solutions and standards will also be researched. Specifically the systems that the Dutch government currently uses or is developing will be analyzed in chapter 2.

Next several design architecture models will be summarized in chapter 3. Specifically, the distribution architecture and key management will be discussed. We will discuss the (dis-)advantages of these architectural approaches and attempt to learn lessons from the design choices of the previously analyzed Dutch government systems.

Finally we will attempt to propose a design that incorporates the lessons learned from this design exploration in chapter 4.

During this research project the lessons learned from the design exploration are leveraged to find an appropriate balance in the delicate equation involving procedural, technological, and sociological variables. During the design exploration we will evaluate if the proposed design meets the government requirements specified on page 3. Further non-government input that influences the design exploration process are more general technical requirements specified in appendix D, and we loosely follow the initial design thoughts specified in appendix E.

1.4.2 Theoretical Limitations

The system outlined in our design proposal is merely theoretical, but should be possible to build with current technologies without restrictive technological barriers or prohibitive cost. For some specific technical details a simple proof of concept may be provided, but these will only serve as an exercise to test theoretical limitations. It is by no means a goal of this research project to build a complete implementation or write comprehensive technical documentation.

Chapter 2

Related Work

In this chapter will outline some forms of government transparency, and look at the relation between transparency and privacy. Of interest is the sociological aspect of trust and how this may depend on transparency, security, and privacy. The principle of *"**privacy by design**"* is also researched.

We will create a summary of related Dutch government technology and standards, some of which are currently in use and some of which are still being developed. The roles of these standards and technological systems in our society are explored, and the subject of their legal and political ramifications will be touched upon. Additionally, the technological standards that have been used to develop these systems are of interest. Through a discussion of the transparency, security, and privacy of existing technology that is currently being employed for government services we hope to learn lessons that can be incorporated in our proposed design.

2.1 Related Research on Government Transparency

2.1.1 Government Transparency in the UK

In 2010 Kieron O'Hara - by request of the Minister for the Cabinet Office - published *"A Report on Privacy and Transparency for the Cabinet Office"*[15]. The report extensively details the issues for privacy of the UK government's transparency programme and offers a set of 14 practical recommendations to the UK Cabinet Office.

Transparency in the context of this UK report and in the Dutch context have a slightly different meaning. The UK transparency report involves the mandatory publication of data collected by public bodies to improve accountability by enabling the people to hold the government to account, as well as other forms of data sharing. The transparency envisioned by the Dutch government is more focused on the right of the individual citizen right to know what data is collected about them personally.

While the kind of transparency in both these countries has a slightly different meaning the risks are similar; the risk of unauthorized use of personally identifiable information equals the risk of personal privacy violation. The importance of privacy to transparency in general is underlined by the conclusion that the public's confidence hinges on this:

> *"Privacy is extremely important to transparency. The political legitimacy of a transparency programme will depend crucially on*

> *its ability to retain public confidence. Privacy protection should therefore be embedded in any transparency programme, rather than bolted on as an afterthought."*[15]

This conclusion seems highly relevant to the Dutch system, since public confidence is an important factor in the Netherlands as well. The Dutch government acknowledges this and is directing efforts to bolster public confidence by maintaining a continuous focus on privacy [10, p.14]. Improving public confidence by focusing on privacy and security was also recommended in multiple studies to help realize the 2017 goals [16][17][18].

O'Hara further concludes that privacy should :

> *"Privacy and transparency are compatible, as long as the former is carefully protected and considered at every stage."*[15]

When developing a transparency enhancing system it is thus imperative that the system is given shape with privacy being protected and considered at every step of the design. To be able to realize privacy safeguards at every stage this process has been formalized in the ***"privacy by design"*** principles.

2.1.2 Government Transparency in the US

A report written by the University of Utah Honors Think Tank in 2012 explored the different facets of both transparency and privacy in their report *"Transparency and Privacy - Clashing Paradigms in a Web 2.0 World"* [19]. The type of transparency discussed covers both the accountability aspect like the UK, as well as the insight in your own data transparency. The honors students acknowledge the delicate balance between government transparency and the need for privacy and security. One of the lessons learned from their report is the concept that these are often opposing interests:

> *"Transparency and privacy are usually inversely proportional. If you become more transparent, you become less private and vice versa"*[19]

This is shown to be especially the case for personal transparency when you no longer have any control over your personal data. With institutional transparency, however, this is not necessarily the case, if transparency is provided with good privacy safeguards. The report summarizes this difference in the following way:

> *"Institutional transparency is generally a good thing; personal transparency not so much much."*[19]

Finally, they also underline the relevance and importance of fostering greater trust in government by enabling government transparency:

> *"The digitization of information, coupled with the ubiquity of the Internet, has enabled government and institutional transparency like never before in our history; Transparency in government operations is the first and most critical step toward fostering greater trust and citizen engagement with our government."*[19]

2.1.3 Privacy by Design Principles

The Canadian Information & Privacy Commissioner (IPC) Ann Cavoukian published extensively on the subject of *"Privacy by Design"*, but the original concept was first described in a 1995 joint publication between the Canadian IPC and the Dutch TNO and *"Registratiekamer"* [1] [20][21][22].

The 7 foundation principles of Privacy by Design can be summarized as:

1. **Proactive** not Reactive; **Preventative** not Remedial. Privacy begins with explicit recognition of the value and benefits of strong privacy practices.

2. Privacy as the **Default**. Data should only be collected and/or used sparingly, with a specified purpose, and with consensual limitations.

3. Privacy **Embedded** into Design. A systemic holistic approach to privacy should bee adopted, and impacts evaluated at every design step.

4. **Full** Functionality – Positive-Sum, not Zero-Sum. Other documented interests should not have to oppose privacy, nor privacy have to compete with these interests.

5. **End-to-End Security** – Lifecycle Protection. Strong security is essential to privacy from start to finish of the lifecycle.

6. Visibility and **Transparency**. Visibility and transparency are needed for accountability, monitoring compliance, and allowing complaints and redress.

7. Respect for **User Privacy**. Individual right to free and specific consent, and access to accurate personal information.

Security is an integral part of the foundation for privacy that should be integrated in the whole lifecycle. Ann Cavoukian advocates the adoption of the *"**Security by Design**"* principles in *"Privacy and Security by Design: An Enterprise Architecture Approach"* [22].

Transparency is another part of the foundation for privacy. Without transparency there can be no accountability, and without accountability privacy compliance can not be monitored:

> *"The collection of personal information entails a duty of care for its protection. Responsibility for all privacy-related policies and procedures shall be documented and communicated as appropriate, and assigned to a specified individual. When transferring personal information to third parties, equivalent privacy protection through contractual or other means shall be secured. [...] Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information shall be made readily available to individuals."* [20][21]

[1] https://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=329

The confidence of the public is of importance for a political success of a transparency enhancing system. Visibility and transparency of the system itself are thus essential to establishing accountability and trust. Giving citizens the ability to verify the systems security and privacy inherently fosters trust. Ann Cavoukian's quote that exemplifies her attitude to trust, in relation to privacy by design, is clear, concise, and to the point:

> ***"Remember, trust but verify!"*** [20][21]

2.2 Related Dutch Technology and Frameworks

In the Netherlands multiple solutions are being combined to satisfy the government's requirements. There are separate solutions for authentication, personal data sharing, and contacting government. Some implementations that we explore are currently in use are STORK, DigiD, eHerkenning, and MijnOverheid. Other explored implementations are still being developed/piloted are eID / Idensys, Digidentity, and Qiy / Dappre. The combination of these systems satisfy some of the requirements stated on page 3. It is part of the government plan to implement all requirements in incremental steps. These steps result in multiple technical standards and implementations, which are strongly interdependent on the required corresponding incremental changes in Dutch law so the legal framework matches the current implementations. For example, the "*Wetgeving Generieke Digitale Infrastructuur*" [9], which is related to these systems, encountered delays because of the large consequences on business processes [23], but will be voted on at the end of 2016 [24].

2.2.1 STORK

STORK[2] is the European standardized framework for trust levels of electronic authentication of individuals. This STORK framework is the basis for the trust model the Dutch government will implement. The trust levels range from 1 to 4 (with 4 being the highest level), and are based on multiple factors including the procedure for verifying identity, and the strength of the security of the authentication mechanism [25, p.17][26, p.20].

Requirements from the European STORK framework are only rough outlines and have proven to be hard to translate into practical use. To aid implementation of the STORK framework in practice, the Dutch Standardisation Forum created better examples and use cases for the standard STORK levels. [25, p.18-26][26, p.21-30]:

- **STORK 1** is the most basic identity without any verification (only e-mail is checked), these can be traditional username and password. This may only be used for unimportant websites, have no legal consequence, and do not show important personal information (BSN is certainly not allowed te be used).
- **STORK 2** has some level of identity verification, requires a second factor, but does not require strong cryptography for authentication.

[2] https://www.eid-stork2.eu/

This may be used for sites with legal consequence, and personal data including BSN may be used.

- **STORK 3** has a high level of identity verification and can provide authentication based on strong cryptography. This STORK level is currently being piloted by the Dutch government in several cities. This authentication level may also be used for *"non-authentic mutations"* in government registries. Mutations of data on the list of specific *"authentic data"* require a higher level of verification because their use is mandated by law for all government agencies[3]. In the Netherlands, authentication levels up to STORK 3 require an identity provider that verifies the authentication, and the recommended open standard SAML is used to communicate this securely [27][28].
- **STORK 4** requires face-to-face identity verification and a strong cryptographic identity verification token (such as a PIV card). Any company can produce the required smart cards, as long as they meet minimum requirements. An example of a new revolutionary smart card that is currently being developed in the Netherlands is the IRMA card, which also offers attribute based identity which is a very useful feature in addition to providing personal identification [4]. This authentication level may also be used for authentic mutations in government registries and to perform actions with the highest economic and public interest.

A strong requirement from the STORK framework is that STORK authentication can be used to access online government services with authentication from another European country. Because the Netherlands participate in the STORK project, all Dutch online authentication providers (DigiD, eHerkenning, or their future replacement in the form of eID / Idensys) will have to support foreign authentication providers.

The legal basis of the STORK framework is being solidified by incorporating it into Dutch law. An example of which are the changes to the the Dutch criminal code law (*"Wetboek van Strafvordering"*) in 2014 which requires at least STORK level 2 for electronic communication with the court, as is currently implemented by DigiD for citizens and eHerkenning for corporations. In the future, this will require at least STORK 3 with STORK 4 issuance procedure (identification and registration in person) [27].

2.2.2 DigiD

DigiD[5] is the current identification provider for citizens in the Netherlands. Technically, DigiD offers username and password with second factor (2FA) SMS authentication for government agencies and business websites. DigiD was a huge step forward because it replaced the multitude of own implementations of authentication mechanisms by the different government agencies. But DigiD is still a fairly low level of trusted authentication, conforming

[3] http://www.digitaleoverheid.nl/onderwerpen/stelselinformatiepunt/stelsel-van-basisregistraties/stelselvoorzieningen/stelselcatalogus/authentieke-gegevens

[4] https://www.irmacard.org/irma-card/

[5] https://www.digid.nl/

only to only STORK level 2 [29, p.11].

DigiD has had security incidents in the past, for example in 2011 when Diginotar was hacked, then both the government root certificate and the DigiD server certificates were revoked causing almost all government online services that depend on DigiD for authentication to become unavailable. This incident is one of the causes that drove the minister to note the urgent need for better security and availability [1, p.5]. Last year it was also discovered that DigiD was vulnerable to phishing attacks by re-registering expired trusted domains from the Dutch police [6].

Security of DigiD relies on basic 2FA, which provides a little more security than only a username and password, but is still an inherently flawed means of authentication which was already obsolete in 2005 [30]. Recent research has shown that 2FA can be defeated just as easily as 1FA when the user's computer has been compromised [31], and these flaws are due to inherent conceptual weaknesses that can only be solved by leveraging secure hardware on mobile platforms for authentication purposes [32].

2.2.3 eHerkenning

eHerkenning[7] is the current identification provider system for businesses in the Netherlands, which replaced the previous DigiD service for businesses in 2011 [33]. Adoption has been slow, in 2013 only 8% of digital government services accepted eHerkenning for authentication, and by 2017 only 85% of all government services are projected to be available online [18].

The eHerkenning system can provide multiple STORK trust levels, some of which are as low as DigiD (which conforms to STORK level 2), but also provides trust levels that are equal to the new eID / Idensys system for applications that require a higher level of trust up to STORK 4. eHerkenning implements the highest STORK level only for applications that require this based on company issued smart cards.

2.2.4 eID / Idensys

The eID system is currently being developed and builds further on technology from eHerkenning, which is being migrated to the eID system [34]. eIDs for citizens was planned as government issued IDs (the DigiD card), but government could not issue these cards before the deadline of 2017 so during the pilot companies tasked by the government will function as identification providers [29, p.19][34, p.4]. After 2017, a higher business interest is expected after leading to a more competitive market for means of identification. Idensys will consist of a federated network of identification providers that provide a higher trust level than is currently offered by DigiD [33].

The trust levels are also based on STORK, but will be the first Dutch system to support the European identity classification system which provides secure identity across borders with multiple levels of trust. The minimum

[6] `http://www.nltimes.nl/2015/02/03/police-website-vulnerable-digid-hack/`

[7] `https://www.eherkenning.nl/`

required level of authentication will be higher than previous authentication systems. The eID / Idensys pilot identity providers will only be allowed to offer STORK level 3 and 4 means of authentication [33].

2.2.5 MijnOverheid

MijnOverheid[8] is a government website that aims to be a centralized portal for handling all government business online. But MijnOverheid consists only of a digital message box that citizens can subscribe to. Messages consist of replacement for regular mail (*"Berichtenbox"*), or specific data that is kept up to date (*"Lopende Zaken"* and *"Mijn Gegevens"*) but these specific data services are not supported everywhere [35]. Citizens can log in using DigiD authentication to read messages, and can configure MijnOverheid to notify them by e-mail when new messages arrive (but not receive this messages in their e-mail for security reasons). Multiple government agencies push messages to the MijnOverheid message box, but when there is a need to respond to these messages or when a citizen wants to make any changes to his/her data, they will be redirected to the separate agency sites and be required to log in with DigiD again.

Agencies can write specific data encoded in UTF-8 ebXML with either eBMS or WUS format directly to MijnOverheid, but in practice the MijnOverheid message box functions as a large digital printer [36][37][38]. Government agencies send a print job over the secure government network when they need to send a letter to a citizen. Normally this job would be printed and mailed by regular mail, but when the citizen is registered as a user of MijnOverheid the print job is stored in the online message box as a PDB (PDF/A-1a ISO 19005-1 with a size restriction of 250 kB per message) [38]. Using well documented document standards is a good method to provide citizens with transparency allowing digital sharing of their documents. However, the system currently provides little more than the information that was previously sent by regular mail - only going as far back as the moment of subscribing - and thus does little to improve transparency.

Because the government recently started a campaign to stimulate registration for MijnOverheid the amount of registered citizens almost doubled over the course of a few months to over 3 million in the beginning of 2016[9]. We occasionally observed some different failure modes that perhaps occurred because of recent scaling issues. Some letters arrive by regular mail, some both online as PDF and by mail, while you would expect the letters to only arrive online as PDF after you subscribe to the MijnOverheid. A hypothetical explanation for these failure modes would be the loss of the message going to MijnOverheid (resulting in a timeout and regular mail being used as the fallback), or loss of the reply with acknowledgement of reception from MijnOverheid (resulting in both the PDF being stored and the fallback mail being used as well). Lost messages are certainly possible by design when either a 'best effort' mode of the ebMS connector or the WUS connector is used to connect to MijnOverheid. Lost messages is one of the known issues

[8] https://mijn.overheid.nl/

[9] https://www.rijksoverheid.nl/actueel/nieuws/2016/01/25/drie-miljoen-mensen-activeren-berichtenbox

that have to be accounted for when connecting to MijnOverheid, for example by rate limiting messages or checking delivery reports [37].

2.2.6 Digidentity

Digidentity[10] is a STORK 3 level authentication provider that is currently being piloted in the Netherlands and the UK[11] and is available to NL and UK citizens as an Android[12] and iOS[13] app. Digidentity requires a small bank transaction, a photo of legal identification (driving license, ID, or passport), and a selfie of the user to be made before a certificate (Digikey) is issued. Finally the phone number is verified by sending a token by Class 0 SMS, which is only displayed on screen by default and is not saved or shared with SMS reading apps without explitly storing the SMS. The registration procedure is documented in appendix G.

Digidentity also offers an additional TOTP authentication mechanism (which is compatible with Google Authenticator)[39]. These mechanisms are cryptographically strong, but key security is very weak. The app developers neglected to use the Android key store facilities, and the app does not check if the device is rooted. Both the TOTP token and the Digikey are stored in an SQLite database, which can easily be dumped from a USB connected computer with the following command:

```
adb shell "su root sqlite3 /data/data/com.digidentity/databases/digidentity
    .dump"
```

This dump contains a table `"totp_codes"` containing the TOTP token which can easily be imported into any TOTP compatible app, as well as a table `"digikeys"` containing the base64 encoded secret. The secret consists of an encoded certificate, a 64 bit nonce, and a 128 bit key. Due to time restrictions the key has not been decrypted, but with a more thorough analysis of the app this will most likely be possible.

The fact that this dump can only be performed with root access is hardly any restriction for an attacker since there are numerous known exploits to gain root access and hundreds of known malicious apps that use these attacks in the wild [40], and despite efforts to secure the platform new generic root exploits are still occasionally found [41].

2.2.7 Qiy / Dappre

Qiy[14] is an open standard for authentication and verified exchange of information. Supposedly Qiy is open, but on a technological level the open standard can not be analyzed since no documentation other than public relations materials which focus highly on governance models are openly available to the public. There are also 12 Qiy principles stated on the website which generally convey a strong pro privacy and individual rights sentiment. The

[10] https://www.digidentity.eu/

[11] https://identityassurance.blog.gov.uk/2014/12/02/digidentity-joins-gov-uk-verify-public-beta/

[12] https://play.google.com/store/apps/details?id=com.digidentity

[13] https://itunes.apple.com/nl/app/digidentity/id916749732

[14] https://www.qiyfoundation.org/

standard is currently being piloted by several Dutch city governments[15], amongst which the hometown of the Qiy Foundation, Boxtel [42]. The first implementation of Qiy is an app named Dappre[16], developed by Digital Me (the software development branch of the Qiy Foundation).

The Dappre website specifies the specific encryption used is standard AES 128-bit CBC with PKCS5 padding[17], and states that "The Qiy Trust Framework dictates the use of RSA and AES 256-bit encryption"[18].
The primary purpose of the app is the sharing of your personal data with other users. This is achieved by linking to another user by scanning a QR code that is valid for 45 minutes. The app also has a built in sharing function to send this QR code containing the secret key over insecure channels such as e-mail. The personal information sharing procedure is documented in appendix H. This QR code contains JSON data with the following fields:

```
{"target":"https:\/\/issuer.digital-me.nl\/issuer\/routes\/
webhook\/c59c34cb-7304-4b50-afe8-c873082b578b","tmpSecret":
"TjYiKKcUdNagt60SWPjj3Q==","identifier":"Thijs Houtenbos"}
```

Both the UUID and the secret change with every new QR code generated. The UUID is thus likely used to uniquely identify the session for the connection attempt using the website as the proxy, and the `"tmpSecret"` is a base64 encoded 128 bit random string that is potentially used as a session key for transport encryption.

When attempting to retrieve the URL listed in the data a certificate error is generated because the website uses a self-signed certificate (technically a certificate signed with a nonexistent Qiy root CA):

```
ERROR: cannot verify issuer.digital-me.nl’s certificate,
issued by ’/C=NL/ST=Noord-Brabant/O=Qiy/OU=Infra/CN=Qiy
Internal Root CA/emailAddress=webmaster@Qiy.nl’:
  Self-signed certificate encountered.
```

The invalid certificate being used on a public facing server could potentially be because this is an early pilot. Also when the observed behavior is by design this does not have to be an issue since this mechanism can still be secure if the app uses certificate pinning of their own CA.

The app also allows dumping of all the data the app has stored with root access. This includes all personal user details, but also other user data that has been transmitted securely via an encrypted channel. All these user’s personal details (name, company, phone, website, email, and photograph) are stored on the mobile device unencrypted and can be dumped by calling:

```
adb shell "su root sqlite3
    /data/data/nl.digital_me.dappre/databases/DappreDB .dump"
```

This personal data from other users also remains on the device if the other user uninstalls their app without explicitly deleting the link between the

[15] http://depilotstarter.vng.nl/burgerregie/persoonlijk-digitaal-domein-de-burger-centraal
[16] https://play.google.com/store/apps/details?id=nl.digital_me.dappre
[17] https://digital-me.nl/consumer/dappre/
[18] https://digital-me.nl/consumer/support/faq/security-and-privacy/

users.

From our test is not apparent if Dappre also uses asymmetric cryptography, it might be that the key is stored in the Android key store. But given that personal other data is stored in plain text, and the app does not check if the device is rooted, it is a moot point so this is not investigated further. The fact that the data is stored as plain text seems to contradict the Qiy principles listed on the Digital Me website, which state that:

> *"Any party who participates in the Qiy Scheme and uses my data or holds them, protects this data in accordance with the requirements imposed on them by the Qiy Foundation."*[19]

The fact that this personal data can easily be read implies that the requirements are either extremely lax, or the app does not adhere to these principles.

2.3 Related Research on Technology

There is a huge body of relevant related research too broad to fully summarize. We shall list a highlight of some of the cryptographic/security standards that are used by existing technological solutions. In the Netherlands any standards that are listed by The Forum Standardization[20] are mandatory (unless a good reason can be stated not to use these when possible). The status of standards in the Netherlands can be checked with a search form on The Forum Standardization website [21]. Some of the following standards may be of interest to a proposed design that we will attempt to construct in this design exploration:

- Personal Identification (PIV) based on standardized model by NIST [43], and compatible with the EU future EID plans [29][44]. Currently some eHerkenning authentication is based on PIV cards.
- RSA is used for asymmetric encryption, this proven standard has existed for almost four decades [45]. RSA is being used by most PKI infrastructure, and according to documentation by the Qiy framework.
- X.509 public key infrastructure certificate standard for exchanging signed certificates, as defined by the IETF in RFC 5280 [46]. HTTPS is based on X.509 and is used by all the researched Dutch government services.
- SAML v2.0 is a standard for authentication and authorisation used to communicate with identification providers in XML format. This standard is recommended by The Forum Standardization [28].
- FIDO U2F is an authentication standard based on asymmetric encryption which can be used universally on any website trough a JavaScript API [47]. The W3C recommends not to wait for the W3C Crypto API to implement U2F but instead develop a generic FIDO alliance

[19] https://digital-me.nl/consumer/qiy-principles/

[20] https://www.forumstandaardisatie.nl/english/

[21] https://lijsten.forumstandaardisatie.nl/lijsten/open-standaarden

authenticator plug-in [48]. U2F technology could potentially be used as STORK 3/4 authentication.

- Key distribution models, either with or without trusted CA and delegation, and their advantages and risks [45][49]. The Dutch PKIoverheid uses a standard trusted CA.
- Databases that supports asynchronous replication and multiversion concurrency control [50] and are eventually consistent [51].
- Secure and private file storage either by maintaining ACLs with a trusted broker [52], or by cryptographic access control without he need for a broker [53]. Storage on untrusted servers with more advanced ACLs can be achieved with attribute-based encryption and (lazy) re-encryption [54], possibly with proxy hosts performing re-encryption without trusted knowledge [55].
- Document exchange should use open formats. The Forum Standardization has a guide to help determine the required standard [56]. For (collaborative) editing the ODF 1.2+ standards is is recommended [57]. For archiving PDF/A-1 must be used when the document does not require incompatible features [58]. For transmission and publishing (and sometimes archiving) of documents PDF 1.7 is recommended [59]. The government service MijnOverheid correctly implements these expert recommendations by requiring letters sent to users to be stored in this PDF/A-1 format.
- HTTP version 2 can be used to multiplex streams over a single connection and to proactively push related files in response to a single request [60].
- DNSSEC can be used to add authentication and integrity to the DNS system using asymmetric keys [61]. NSEC3 records add authenticated denial of existence to the DNS system as well [62].
- Password based key derivation algorithms should be used when expanding a user entered password or authentication token to a crytptographic key. NIST recommends the use of PBKDF2 for this purpose [63]. Modern algorithms such as Scrypt are hardened by requiring more memory, not hindering normal operation but making brute force attacks with custom hardware harder [64].
- Hash based message authentication (HMAC) provides message authentication based on a cryptographic hash and a secret key [65]. Additionally and HMAC can be used for authentication by returning the HMAC for a given nonce proving posession of the secret key.

2.4 Evaluation of Related Work

Public confidence in transparency enhancing technology relies on a strong focus on privacy. The relation between transparency and privacy can be summarized as symbiotic because transparency relies on strong privacy, and good privacy relies on transparency. Privacy further depends strongly on security, when security is broken personal privacy is compromised. To safeguard a secure and privacy respecting transparency system the design should be create in accordance with *"**Privacy by Design**"* and *"**Security by Design**"* principles. Both these sets of principles suggest the minimal amount of trust needed should be given by design, and the general guidelines of *"**Minimal Trust**"* and *"**Trust but Verify**"* should apply.

Our exploration of existing Dutch government systems seems to indicate that they do not yet satisfy all the requirements outlined on page 3. The ambitious goals of the government in regard to enhancing transparency have not yet been met. The only system aimed at enhancing transparency is MijnOverheid, and the amount of transparency offered is currently insufficient. Most effort seems to have been focused on the development of stronger authentication infrastructure. It is however our opinion that steps are being taken in the right direction with current and future developments. Replacing DigiD and eHerkenning with the eID / Idensys system will most likely increase the system security and privacy, both of which are required for transparency enhancing technology. A missed opportunity is the current lack of a previously envisioned DigiD card that could have provided the strong authentication mechanism required for a transparency enhancing system. The new Digidentity mobile app based authentication mechanism that is being piloted as a workaround for the lack of these physical cards is inherently less secure. Security issues we identified with this app may allow the second factor authentication to be bypassed by an attacker entirely, reducing the security to below the current basic 2FA that DigiD offers. Digidentity now provides a false sense of a higher level of security, while it in fact offers a much lower level of security. Digidentity is not the only app that does not meet expectations. The other app we evaluated is Dappre, the first implementation of the Qiy Framework. While the Qiy framework could potentially be leveraged as the basis for transparency enhancing technology, not enough details of this supposedly open standard are public to confidently conclude anything based on specifications. The implementation the form of the Dappre app, however, does not meet our expectations of privacy, and thus provides a false sense of privacy. Issues like this may reduce the confidence of the people in the security and privacy offered by the government, making it harder to gain the trust of the public later.

These two apps illustrate an apparent issue with developing new (mobile) platforms for authentication; the design could be technologically feasible, but the practical implementation of the technology is not well designed. There is no lack of available standards and technology, and sufficient effort seems to be invested into the design. However the balance between the procedural, technological, and sociological areas of the design process seems to have skewed to the procedural and sociological as evidenced by the abundance of documentation in this area. This might be influenced by the strong bureaucratic and inherently political nature of design processes involving government. The technological design should be equally well documented and be open and transparent. By not fully opening the technological parts of the design process the principles of *"Privacy by Design"* and *"Security by Design"* may be violated. In practice this may lead to implementation shortcomings of otherwise good designs.

Chapter 3

Comparison of Architectures

In this chapter we shall compare several different distribution architectures that could be used for transparency enhancing technology. The level of (de-)centralization of the system is relevant to the trust model and the inherent privacy risks those involve. We will compare scenario's with the most centralization (a fully centralized system on one logical trusted server), and the most decentralized (a fully peer-to-peer with no single privileged party). By analysing the strengths and weaknesses of both extremes we will attempt to find a middle ground. Our aim here is to provide a potential solution that balances the level of (de-)centralization. To balance this we must weigh the transparency, security, and privacy requirements that are implicit to the architectural design. Different architectures can of course be combined in this process. A potential solution could consist of a federated architecture where users can choose where their (meta)data is stored, but which still requires several centralized servers and privileges to make this work in practice.

The distribution architecture is also important for the architectural capabilities and requirements of key management. We will outline some different scenarios involving the locations where cryptographic keys can be stored based on architectural choices. The potential security and privacy implications of the location of the keys will be noted. We will also outline how cryptographic signing/verification/encryption/decryption could be performed with these scenarios.

3.1 Distribution Architecture

The distribution architecture of the system includes the location of servers that provide the service, where the user (meta)data is stored, and traffic flows. The level of centralization of this system can take many forms with distinct (dis-)advantages. These different levels are (more or less) mutually exclusive, making the choice of level of centralization a defining factor for laying the foundation for the system design.

3.1.1 Centralized

A fully centralized system has a single central service (with one or more central servers) managed by a single entity. All parties connect to this single service, as is illustrated in figure 3.1. An example of this is the existing MijnOverheid. Advantages of a centralized model are technical and operational simplicity, and ultimate trust in only one party is needed. Disadvantages are that you place all your trust in one party which has control over all (meta-)data, creating a high value target for attacks, and having a single point of failure reducing the system robustness.

Government systems with a centralized architecture include DigiD, MijnOverheid, and PKIoverheid. The Qiy framework implementation Dappre is also a centralized system, relying on the central service for communication and implementing their own CA for signing certificates. Some of the issues that occur in practice with these centralized systems are a direct consequence of their centralized architecture. An example of this is the unavailability of all government services depending on DigiD when the Diginotar incident occurred as was described on page 10.

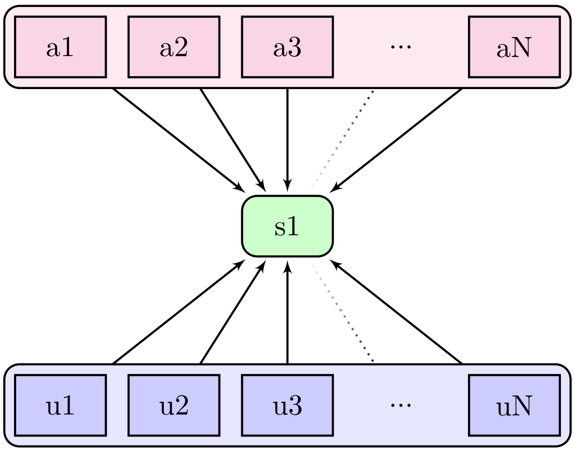


Figure 3.1: A centralized architecture with both agencies a1-aN and users u1-uN writing to and reading from the same central service

3.1.2 Decentralized

A fully decentralized system has no central servers and limited means of control over the entire system by any single entity. The system consists of a network of both data producing and data consuming nodes, as is illustrated in figure 3.2. In this network, both agencies and users are peers that communicate directly with other peers (P2P). This system can either function with a distributed model or even a trustless model. An advantage of this system is the fully distributed nature of this system, not requiring any trust anchor or privileged party.

Distributed trust model

The PGP web of trust is an example of a fully distributed trust model. A party can personally indicate their trust in another party, and this trust can be inherited by trusting the trusted parties of another ultimately trusted party. An advantage of the distributed trust model is that there is no default trust, so all trust relations are explicitly defined by the user. This PGP web of trust is also known as the '*anarchy*' model [66].

Another example of a distributed trust model is currently being piloted by Whitebox Systems[1]. Specific medical data is securely shared only after

[1] https://hka-pilot.nl/

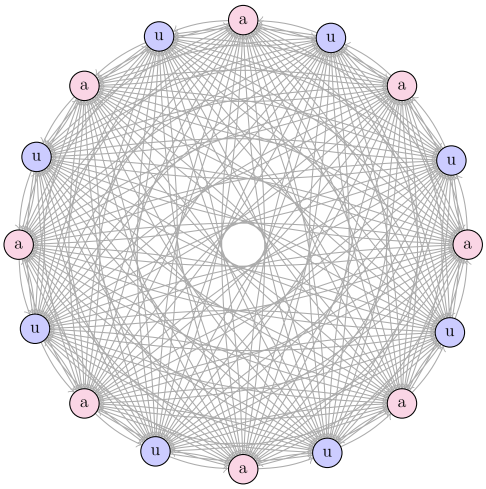


Figure 3.2: A decentralized architecture consisting of a network where all agencies and user are peers and connect to each other directly

the patient provides explicit permission to their physician. Physicians explicitly shares patient data with other health care professionals who have a treatment relationship with the patient. The boundaries of trust in this model correspond to the real world 'natural' boundaries of health care treatment relationships [67].

Trustless P2P model

The Blockchain used to store Bitcoin transactions is an example of a fully trustless model. An advantage of the trustless P2P model is reliance on cryptographically and computational principles to create permissionless trust which is publicly verifiable by anyone. Disadvantages are the computational complexity and the large storage required for all nodes to store the entire blockchain to be able to verify all the whole system. This last disadvantage is highly restrictive for use on mobile devices, requiring trust in third parties to perform validation to allow mobile use. For the purpose of a transparency enhancing system for government a lack of incentives to perform computation in the network may create an additional disadvantage that there is a limited amount of control over the network, and adversaries may compromise the network with a moderate amount of computational power.

3.1.3 Federated

A federated architecture consists of a network of heterogeneous services owned by multiple entities with some degree of trust between the services, as shown in figure 3.3. A defining characteristic is the segmentation of ownership, with no single entity controlling a majority of services. This is closer to a centralized service than a decentralized system, a difference being that this is a subdivided network where each entity offers their own central service. An advantage of a federated model is granting the users a choice which entity they trust with their (meta-)data, stimulating competition between organizations. This choice is important in the case of the compromise of part of the network, because of the heterogeneous nature of the different services only a part of the users will be affected. This segmentation of the network is a defining characteristic of a federated network that sets it apart from both fully centralized and homogeneous distributed architectures. A disadvantage is having a certain level of trust in a multitude of entities. The disastrous consequences of trusting to many entities are demonstrated in practice by the amount of security incidents with the Public Key Infrastructure, in this case because of the plethora of trusted CAs. Another potential disadvantage of a heterogeneous network can be integration issues and network inertia, which can contribute to slower roll-outs of future updates because compatibility in the network needs to be maintained.

Government systems with a federated architecture design include eID / Idensys and by extension implementations such as Digidentity.

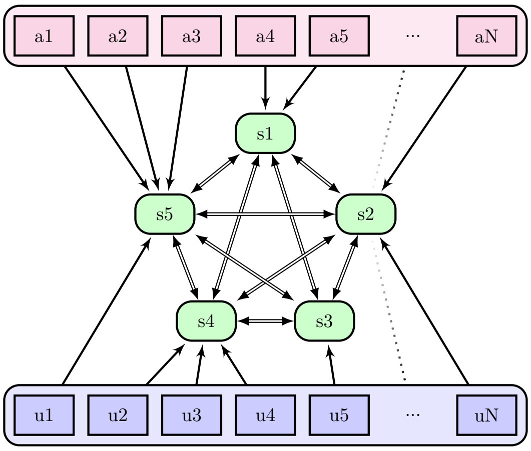


FIGURE 3.3: A federated architecture consists of a network of trusted services where each agency a1-aN and user u1-uN makes use of at least one service

3.2 Key Management

Key management architectural choices depend largely on the distribution architecture. The architecture choices involve the key issuance procedure, the location where keys are stored, and the location where encryption/decryption/signing is performed. We compare the options for these locations available for an online application. Multiple key management designs can potentially be combined for compatibility.

3.2.1 Central Server

Keys stored on (a trusted key store in) a central trusted server. An advantage is that the server can perform operations on encrypted data on behalf of the users. A disadvantage is that data encryption does not protect against unauthorised access to the server. Additionally a much higher level of trust in the central server is required, which has full access to all encrypted data. Transparent disk or database encryption is an example of encryption that is used on servers.

3.2.2 On the Local Computer

Keys are stored in a trusted key store, possibly encrypted with an additional password. Secure software will need to be installed to manage this key store, preferably on the OS level. For a higher level of security a dedicated machine can be used, or for the highest level of security even an 'air gapped' machine could be used for offline signing. An advantage of storing keys on the computer is the fairly good balance between user control, ease of use, and the level security. A disadvantage is that portability to other machines is not convenient, but this could be made convenient by storing the encrypted certificate on a central location for easy transfer. When the certificate is protected by a sufficiently strong password, or stored in a key store that prevents a brute force search this can be secure. Brute force searches can be prevented by rate limiting the number of attempts, require a secondary password or PUK code, or erase the private key after a number of failed attempts.

3.2.3 On a Smart Phone

Keys are stored in a trusted key store, possibly encrypted with an additional password/PIN/fingerprint. This requires secure installed apps that verify platform security, and for the highest security a dedicated mobile device (reducing risk of other apps that may contain malware). Portability is high, allowing certificates to be installed by following a wizard and/or scanning a QR code. This is the mechanism used by mobile app based authentication providers like Digidentity[2] and QIY (specifically the Dappre app[3]) uses to authenticate users. Mobile platforms such as Android[4] and iOS[5] provide a fairly secure key store that is separated from the main OS with support for strong cryptography. Even users or malicious apps with root access should not be able to access keys stored in the key store. The use of mobile platforms for secure authentication could be possible by relying on secure hardware [32]. Secure hardware can perform the functions of the key store with an even stronger separation from the rest of the hardware and software of the mobile system.

3.2.4 With a Smart Card

Keys are stored in a hardware cryptographic chip on the smart card (or other PIV card). An advantage of the secure hardware is that the keys can be guaranteed to be stored securely (keys can never be exported from the smart card chip). Keys do not need to leave the chip because all required cryptographic operations are implemented on the chip and can be called trough an API after authenticating with a PIN. A disadvantage is that the PIV has to be read with a smart card reader, NFC connection, or direct USB token connection. Also the PIV can get lost easily, so an easy replacement mechanism must be in place. Another disadvantage is the slow speed at which the token can perform decryption/signing, which was over 300 times

[2] https://www.digidentity.eu/

[3] https://digital-me.nl/business/ready-to-use-software/dappre/

[4] http://developer.android.com/training/articles/keystore.html

[5] https://developer.apple.com/library/mac/documentation/Security/Conceptual/keychainServConcepts/02concepts/concepts.html

slower as indicated by our benchmark listed in appendix F. When the volume of signatures and decryption is manageable this method is feasible and offers the best security by far.

3.2.5 In the Browser

Key storage in the browser is is possible, but a more secure solution would require encrypted keys stored on a central server, or perhaps even directly on a smart card. The user logs in and downloads the certificate which is then decrypted and used for further authentication, decryption, and signing. This solution should only be used for backwards compatibility, since it does not offer the level of protection other solutions do (because of the risk of keys being intercepted in the inherently insecure browser environment). Performance wise performing encryption in Java Script is feasible [68], and there are good cryptography library implementations available such as CryptoJS[6]. We confirmed a relatively good performance factor of 1.5 to 7 times slower than native CPU performance in our benchmark listed in appendix F.

The W3C is currently working on the Web Cryptography API[7], which will be much more secure than the native JS implementation but there are still some issues that need to be solved [69]. An alternative requiring browser a plug-in to directly access smart card is possible, a disadvantage of plug-ins is that there are no good standard solutions available and installing custom software this might not be the most secure option because it may offer new attack vectors [70]. An option that worked well until recently was using a Java plug-in to access the smart card from the browser, but this has become so cumbersome that it no longer is a viable option[8]. FIDO U2F could also be used as universal second factor authentication. Because of the strong backing from an alliance and given the availability of working plug-ins the W3C recommends not waiting for the W3C Crypto API to implement U2F [48].

When backwards compatibility with alternate authentication that only guarantee a unique token for each user has to be implemented, a solution would be to store a private key as an strongly encrypted blob on the server. After using the backwards compatible authentication to log in to the system the blob is sent to the client side application browser. The client software will ask for an additional key password/PIN to decrypt the key before performing signing/decryption operations. A disadvantage of this method when compared with using the key store on a mobile platform is that the key can be attempted to be brute forced when the browser has been compromised. Unlike the key store there will be no protection that will prevent multiple repeated attempts. A strong password requirement and a key derivation algorithm with many rounds can be used to mitigate this by making brute forcing of the key unfeasible. When the key has been decrypted it can also be read from memory for the duration of the operation.

[6] https://github.com/sytelus/CryptoJS

[7] https://www.w3.org/TR/WebCryptoAPI/

[8] https://www.w3.org/2012/webcrypto/webcrypto-next-workshop/papers/Using_the_W3C_WebCrypto_API_for_Document_Signing.html

3.3 Discussion of Architectures

We performed a high level privacy and usability evaluation of the architectural choices for a transparency enhancing system. We considered the requirements listed on page 3 with an additional focus on the principles of *"privacy by design"* and *"security by design"*. Given these requirements and principles it seems most promising to use a federated architecture for our design.

The fully centralized system is entirely unable to fulfill the requirements, requiring too much ultimate trust in one single party which has proven to be misplaced in the past. Current centralized systems are being replaced with federated successors (such as is the case with DigD and eIdentity being replaced by eID / Idensys). Federated architecture is also being mandated by the EU for identification providers. Building a centralized system on top of this only serves as an unnecessary abstraction (although this may be used to provide backwards compatibility for older systems that rely on one centralized party to perform their authentication).

The fully distributed system is most likely too cumbersome to use for this design exploration. An anarchy based distributed trust model may work for situations with personal trust and face-to-face contact such as with health care providers, we do not deem this model suitable for a transparency enhancing system. It is not practically feasible to manage trust relationships between government agencies and citizens without either a high burden of physical key exchange or some form of centralized directory service. The fully trustless P2P model does however have the added value of a fully distributed verifiable ledgers like the block chain. Such a public ledger could be used to implement a public directory database because it provides excellent open accountability.

For key management there is one location for storing keys that is superior to all others; the smart card. This is the only location that does not allow the key to be compromised and yet provides strong cryptographic authentication. The inability to conveniently utilize a smart card with an online service is however a huge setback for online security, especially since previous capabilities are no longer viable. Combined with the fact that the Dutch government will not issue the DigiD cards in the near future another method will need to be used that provides forward compatibility with a future smart card based authentication mechanism. Using a mobile app as a capable smart card replacement - a *"smart card app"* - seems the best option at this point.

The Digidentity app uses the smart card replacement approach, but fails to use the full security features available from the platform. When this app is implemented correctly by using the more secure key store it can provide the high level of security and privacy required for transparency enhancing technology. When using a *"smart card app"* in conjunction with a website using the app as a 2FA is relatively easy to implement. Signing requests should not prove to be a hard problem either, the phone could scan a QR code to obtain a reference to the exact data and prompt the user to confirm his/her signature before submitting the signed message to the server again. To be able to securely decrypt data for use in the website is a much harder problem to solve though. All data that has to be decrypted will essentially have to be proxied trough the app. Data will either have to pass trough the server again unencrypted (defeating the purpose of the privacy features), or a complex mechanism will have to be constructed to re-encrypt data with another temporary session key to allow decryption in the browser. This problem may be harder to solve but can likely be solved with an efficient cryptographic solution.

Chapter 4

Design

In this chapter we attempt to provide a satisfying solution to the question: How could transparency enhancing technology be designed for use by the government without negatively impacting citizen privacy?

Our proposed solution consists of a federated system architecture with a high degree of distribution freedom. A person has a choice where his/her personal (meta)data is stored, and can decide who have access to their data.

We first explore a procedural solution together with the social aspects of the design. These two factors determine a persons experience of the system, and by relating those to familiar social experiences we allow the user to more readily appropriate the system. After this we discuss a possible feasible technical solution.

4.1 Proposed Procedural Solutions

The procedures used to implement this system are designed to closely mimic natural social experiences. Analogies to recognisable real world constructs are made to illustrate the psychological connection.

4.1.1 Credential Issuance

At least once do your personal credentials have to be verified in person to insure the identity you are online does in fact represent you. For this purpose you psychically visit a government office or other official identity provider, this can be any identity provider that meets the minimum government requirements. Your identification papers are verified thoroughly by an identity official. The official signs a certificate stating that you have appeared before him/her and personally validates your digital identity, ensuring that you can henceforth be identified with your new personal key. The official then creates your personal digital vault that only unlocks with your personal key that is handed to you personally by the identity official (for example in the form of a new eID card).

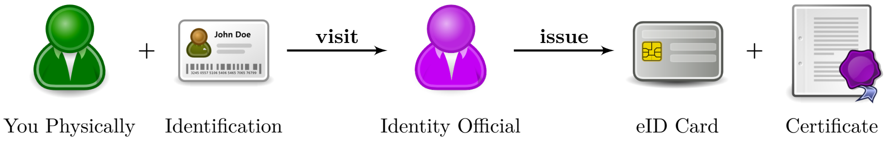


Figure 4.1: An eID card is issued to you physically by the identity official that certifies it

Figure 4.1 shows the regular procedure of issuing an eID card by an identity official. Alternatively you could buy your own smart card that meets the eID specification minimum requirements and have this registered by following roughly the same procedure as shown in figure 4.2.

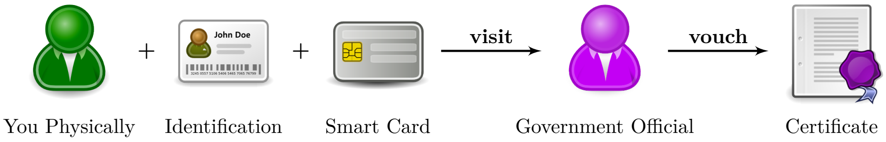


FIGURE 4.2: Another smart card is registered and certified by an identity official

The identity official neither acts merely as a natural person, nor merely an extension of the identity provider organization. It is thus neither correct to use the identity of a natural person, nor to use the identity of the organisation for the purpose of certifying identity. The identity that is used to sign your personal certificate should be the authorized personal identity official in his/her official work capacity. The identity official can thus be held accountable for identity fraud while in his/her official capacity in the case that digital identities have been maliciously or negligently issued. There is no need for the identity official key used for signing certificates to leave the identity provider office premises, resulting in strong physical security procedures of the keys.

4.1.2 Personal Home Service

Your personal home service is the digital vault contains your personal (meta-)data. Not only the content of the records is privacy sensitive information but also the labels on the outside, who has access to these records, and the usage patterns. Just like a person can choose which bank they trust to best ensure their security and maintain confidentiality to respect their privacy when renting a physical vault should the person be able to decide the service where their digital vault is located. A person discloses the location of their digital vault to any party they want to allow to locate it. To allow agencies to deliver a message to your main vault you make the location known in the public directory by signing a certificate that states this location. Just like you can rent additional vaults at competing banks you should be able to have additional digital vaults. You can choose to make the location of additional digital vaults known to only the parties that need to know about these vaults. The owner of the vault shares an Access Control List (ACL) with their home service, specifying which parties can open their vault (provided they have the key as well), or add new files to the vault. The authorization of the vault is thus verified by the personal home service, to further bolder security in addition to the lock and key mechanism in place. Each personal home service should take the best possible precautions to insure the privacy, confidentiality and security of their users.

4.1.3 Public directory

Beside the multiple personal home services there is a single public directory with the function to allow you to locate a person or agency in the federated network. When you need to contact a person their public contact details can be looked up in the public directory. A persons officially verified online identity can be found so you know you are contacting the correct person. To be able to verify this identity you must be able to verify the identity of the official that signed the certificate. Additionally, the location of any person's main digital vault can be found in the public directory. The public directory can thus compared to a phone book with your official phone number listed, but any additional secret phone numbers are not listed under your name.

4.1.4 Namespaces

Your different digital vaults all have separate agencies and people that you have granted access. Some large vaults might even have another small vault inside that only some people can access. Each vault can have a name label, the large vault could for example be labelled *"tax records"*, and the small vault inside *"income 2015"*. Each vault is thus a namespace that can contain further namespaces with some logical inheritance of the type of records contained in it. These namespaces represent natural social permission boundaries, with specific actions granted to the people that have access to the namespace. You might allow your accountant to read all records inside your *"tax records/income 2015"* namespace, but only allow modifications to the namespace *"tax records/income 2015/returns"*. Granting and later revoking access to a namespace can be compared to giving a copy of the key of a vault to a person and later changing the lock (not forgetting to give all other parties with access a new copy). When access is revoked to a party you no longer wish to trust, further information from the vault should be not allowed to be known by this party. The only information that can potentially be known by a formerly trusted party are the records that have previously been viewed (and perhaps copied without your knowledge).

4.1.5 Pseudonyms

Many physical government services - and certainly services offered by businesses - do not require personal identification. When making use of these services digitally this should naturally remain a possibility to protect your privacy. To be able to make both secure and anonymous use of services pseudonyms can be used. But for official business the need for legal recourse might warrant the need to identify a person, for example in the case that a person violates laws or contracts are not honored. To allow anonymous use of these services and still allow a person to be identified by the courts when needed a trusted third party is needed to keep a confidential register of links between the persons identity and their pseudonyms. Anonymity towards the services is preserved unless otherwise ordered by a judge. This link register is a special service offered by the government. When I send a signed certificate to the link register proving that a certain pseudonym is me, the link register returns a signed certificate stating that they know the identity of the pseudonym, and that they can identify this person for legal purposes should the need arise. Pseudonyms can also create anonymous namespaces that can not publicly be linked to your main identity. Anonymous namespaces could be compared to a locker found at the train station.

4.1.6 Lost identity

When losing a single key to your physical vault you would go to your bank, identify yourself and request a change of the lock on the vault to prevent potential unauthorised access when someone would find the key and figure out the location of your vault. The lock to your namespaces can be changed in the same way by revoking the lost key, as long as you can still authenticate as your digital identity. However, when you lost all means of authenticating yourself as your digital identity that identity is considered lost. There is no more use to continue using a locked vault that can not be opened anymore, and since there might be a risk that someone finds the keys to your vault you want to make sure the old vault is not accessible anymore. The procedure for creating a new identity with a new namespace is the same as the credential issuance procedure described on page 26, with the addition that the identity official also revokes your lost key permanently locking your old namespace. To prevent new data to still be added to the lost namespaces the old namespace should be unlisted from the public directory and the home should verify that the owner key is still valid before accepting writes.

Because of the urgency of locking the old namespace when the key has been lost it is not advisable to wait until the time that a person can physically visit their identity provider for re-issuance. To facilitate a faster disaster response there should be an option to remotely request the namespace and key to be put under temporary lock - a re-issuance freeze period - for a reasonable period pending the physical identity check. This can be compared to the procedure of reporting an ATM card lost by telephone (with questions serving as alternate weaker identity verification), but requiring personal identification during the physical pickup of a new ATM card at the post office.

4.2 Proposed Technical Solutions

The technical implementation of the proposed design relies on heavily strong cryptography, most significantly asymmetric cryptography, but also symmetric cryptography, and cryptographic hashes. Our design is founded upon *"privacy and security by design"* principles by leveraging a multitude of strong encryption keys, leading to our proposed design to be introduced by differentiating the cryptographic keys used in the design. Firstly, asymmetric keys used for authentication and verification for each party and component in the system design are listed on page 29. Secondly, different symmetric keys used for encrypting namespaces are listed on page 33. Thirdly, technical namespace design building on these cryptographic keys is further expanded upon on page 35. Fourthly the encryption and storage of records in the namespaces is elaborated on page 39. Lastly, some possible failure modes due to compromise of specific keys are explored on page 42.

4.2.1 Asymmetric Keys

Each user needs to be issued a primary key pair that is registered to their name, preferably in the form of a STORK 4 smart card (or other means of authentication) containing 3 key pairs for authentication, signing, and decrypting. When an unspecified user key is mentioned in this report it will generally mean the set of these 3 key pairs. For the purpose of this theoretical design user keys with a minimum strength of RSA 2048 are assumed.

Types of Asymmetric Keys Used

- **CA key pair**, a CA key pair that is allowed to sign (government) official and service keys (PKIoverheid root CA certificate). These root certificates have a very long active lifetime and will thus have expiration dates well over a decade into the future.
- **Trusted root key pair**, the key that is the owner of the root namespace. This key should also have a very long active lifetime.
- **Service key pair**, a key pair specifically issued with a HTTPS EV certificate marked for use in this system (PKIoverheid EV certificate). These certificates should never be valid for more than 3 years, and be renewed with new private keys every year per industry standards [71]
- **(Government) official key pair**, a personally registered (government) official key that is used to sign user keys (PKIoverheid personal certificate). These certificates have a short active life but an expiration date that is relatively far in the future.
- **Primary identity key pair**, the key pairs contained in a smart card that are personally signed by a identity official after face-to-face identification (for example: PKIoverheid personal certificate). The card should contain separate key pairs for authentication, signing, and encryption. These keys should have an expiration date that is both practical and secure.
- **Additional identity key pair**, additional key pairs that are signed by the users primary key pair (this can be any certificate type). These key pairs can be publicly visible aliases or pseudonyms that are not visibly linked to the primary key.

Public Key Directory

The public directory contains the list of registered public keys with their associated key IDs and the certificate that confirms their identity. Additionally, revocation certificates are also stored when needed, these are either signed by another user key or by an official in the case of loss of all user keys as is further described on page 32.

In the example listed in table 4.1 the user12345 key is signed by the official678, which is in turn verified by the PKIoverheid CA. The alias12345 is an additional user key pair that is a known alias since everyone can see the inheritance relation in the public directory. The pseudo12345 key, however, is a pseudonym of user12345 which is signed by the link register. The use of pseudonym namespaces is further explained on page 38. A user can create a new subkey as an alias of a primary key by publishing this signed key in the public key directory as shown in the following pseudocode:

```
alias12345 = GenerateKeypair()
Directory.Keys.Add(Sign(user12345,{
```

Key ID	Signature	Key	Revocation
trusted root	CA	F00F00F00F00	-
link register	CA	C0DEC0DEC0DE	-
official678	CA	BADBADBADBAD	-
user12345	official678	053053053053	-
alias12345	user12345	BADA55BADA55	-
pseudo12345	link register	133713371337	-
oldalias	user12345	100000000001	user12345

TABLE 4.1: Examples of keys stored in the public directory

```
    "id":alias12345,
    "signature":Sign(user12345,"I hereby certify alias12345"),
    "key":alias12345.Public
})
```

Users should also be able to register additional primary keys by certifying their own secondary smart card with the same process as registering an additional subkey. A schematic represntation of this process is shown in figure 4.3.

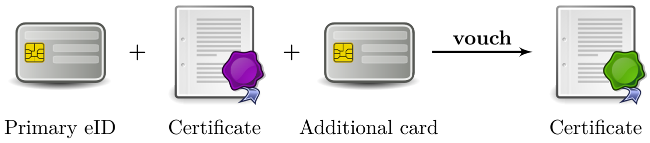


FIGURE 4.3: Another smart card is registered and certified by an identity official

Key Expiration and Renewal

All keys have standard PKI expiration dates that correspond with the key size, cipher and the assigned use of the keys. Keys must be renewed before the expiration date passes to allow secure operation to continue uninterrupted. For practical reasons the primary identity key pair should be of sufficient strength that the key can be used for several years. There should, however, not be any issue with regular (more often than yearly) key renewal when the users themselves can generate a new key, sign the new key with the old key, and revoke the old key. When government, however, demands that identity providers verify the new key in person key renewal periods larger than one year should be used instead.

Renewing a key is possible without interruption, data loss, and has near instantaneous effect. When replacing the old key all certificates signed by the old key should be re-signed with the new key to extend their life as well, for example the certificates that are listed in the public key directory or the public namespace directory described on page 35. The user key renewal process in pseudocode works as follows (details for reading and writing of keys and certificates to the public directory and the home service are omitted in this example):

```
new_key = GenerateKeypair()
```

```
certificate = Sign(old_key, "I hereby certify new_key")
for each old_certificate signed with old_key:
    new_certificate = Sign(new_key, old_certificate)
revocation = Sign(new_key, "I hereby revoke old_key")
```

The role of the new key depends on the role of the old key. A new key signed by the owner key of a subnamespace can only be used in that subnamespace, and likewise a new pseudonym key signed by an old pseudonym can only be used in the context of the pseudonym namespace. Only when the key is signed by the primary key - which is the owner of the user root namespace - can it be used as a new primary user key. Namespaces are further specified on page 35 and pseudonyms are specified on page 38.

Key Revocation When a Key is Compromised

If the user has/had multiple authorised (primary) keys another still uncompromised primary key can be used to revoke the key that was compromised. Additionally, a new key can be issued as is described in the key expiration process outlined on page 31.

If the last user primary key has been compromised the user must follow the lost identity procedure outlined on page 28, resulting in new credentials to be issued as is outlined in the credentials issuance procedure on page 26. The results of this procedure will be visible in the public key directory as the following two rows:

Key ID	Signature	Key	Revocation
user12345	official678	053053053053	official123
user12345.2	official123	A55A55A55A55	-

Table 4.2: Example result a key re-issuance

The namespace directory will only contain one reference to the user, with the new key id specified as the owner. Finding the user namespace will be unambiguous, as is detecting the revocation of the old key. Furthermore, the process has accountability since it the identity official that performed the re-issuance can be identified by anyone in the public key directory. This model with key revocations stored in the pubic key directory resembles a key revocation list (CRL). A CRL chosen over an alternate solution like OCSP - which is now preferred for HTTPS PKI certificate revocation checking - because there is no need to contact a specific CA and have them sign a confirmation of the certificates validity in a closed system. In this design the user should be the one that has final say in their certificate validity, and only when the user is entirely unable to perform any operation on their namespace may this revocation ever be issued by an identity official. Abuse of this is equal to identity fraud, likely causing the identity official to lose their job and perhaps face prosecution. Furthermore, identity fraud like this is highly detectable because it is not possible that users can continue to use the system after their namespace has been re-issued.

Because the user starts with an empty new namespace this may result in data loss. In the context of a transparency enhancing system it is, however, expected that the data shared by the agencies will still be available to them.

When agencies re-establish a trusted relation with the user they can therefore resent all data to their assigned namespace, this will cause the namespaces to be rebuilt from the copies of agency data. This procedure may not be instantaneous, but when agency databases keep copies of all data the user namespaces may be fully restored eventually.

Early End of Active Life

Identity official keys require a more frequent rotation to mitigate impact in case of compromise, and to prevent expiration of the signing identity official key before the user keys that are signed expire. When user keys have an expiration date N years into the future, the identity official keys must have a lifetime $M < N$, and an expiration of $N + M$ years into the future. Additionally, the identity official keys have a limit of K signatures which also helps limit the impact in case of compromise. When the active life of the key has ended no new signatures should be accepted as valid, and the key should be stored in cold storage or destroyed. The signatures and public key remain available in the public directory and are still valid until the expiration date which is after all signed keys have expired as well.

A practical workable example would be the values: $N = 24 months, M = 6 months, K = 1000 keys$. This means that the the government official key is valid for 30 months, but can only actively be used to sign keys for a maximum of 6 months or a 1000 keys signed. With these example numbers the key signing count will most likely always be the limiting factor (for a busy identity officer in the order of weeks instead of months), requiring more frequent Identity Official key renewal.

4.2.2 Symmetric keys

Each namespace contains multiple keys that give a different level of access to the namespace.

Types of Symmetric Keys Used

- **Namespace lookup key** is used to find the namespace and the home service location in the public directory. When this key is shared with agencies or users they will be able to locate the namespace home service. Sharing this key corresponds with the right to locate a namespace.

- **Namespace metadata key** is used to decrypt the namespace metadata such as record listings and other metadata on records. When this key is shared with agencies or users they will be able to list the files and folders that are available in the namespace. Sharing this key corresponds with the right to list records and read metadata.

- **Namespace write key** is used to authenticate a write operation. The write key is used to calculate message authentication proving the message is sent by a party with write access. Sharing this key corresponds with the right to write record metadata, and is needed in conjunction with the namespace master record key to write record content.

- **Namespace master record key** is used to decrypt the individual record keys. When the master record key is shared with agencies or users they will be able to read record keys to be able to decrypt a stored record (and write in conjunction with the namespace write key). Sharing this key corresponds with the right to read records, and is also needed in conjunction with the namespace write key to write records.

- **Record key** is the key that is only used for one individual record. When an individual record key key is shared with agencies or users they can decrypt the single associated record. Sharing this record key corresponds with the right to read the content of a single record (only the file blob, not the metadata).

The combination of these keys can give fine-grained access rights to a user or agency within the namespace. By withholding/sharing these keys the user can restrict/grant rights to lookup the namespace, list records, write records, read all records, and read an individual record. When using 256 bit encryption keys the required storage space for the 4 namespace keys would be $4 \times 256 bit = 1024 bit = 128 byte$ per key pair that grants access to the namespace. These keys are separately encrypted with the public key of each party in the ACL that have been granted access by the user as shown in figure 4.4. These users each receive and decrypt their namespace keys with their private key and can use these to access the namespace. A party can have multiple primary keys, in this case they can choose to re-encrypt these symmetric namespace keys for storage on their home service. It is, however, never allowed to store these namespace keys unencrypted anywhere.

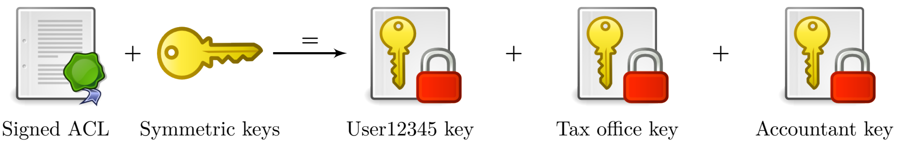


FIGURE 4.4: Namespace keys are encrypted with the public keys of multiple parties

Namespace Key Expiration

Symmetric keys typically do not expire, once a record has been stored with one encryption key this remains static. Re-encrypting with a new key seems to serve little purpose because the amount of time it takes to break the first key remains the same and the goal of obtaining the plain text can be achieved in the same time. Unlike with asymmetric cryptography one key is not reused as often, certainly not with the same IV. There are, however, some cases to be made to let symmetric keys expire:

- If keys are reused many times for a long time (like some namespace keys are) successfully completing a brute force attack on the oldest record in the namespace would enable an attacker to read the newest records as well.

- If keys that have been compromised without being detected will never be replaced it allows an attacker to read all records for a long period of time.

- Deprecated cryptographic algorithms can be phased out much faster by updating keys using a new algorithm, increasing the future-proofing of the system.
- Key strength can also regularly be increased as a matter of normal operational procedure.

In this proposed system design all 4 namespace keys should regularly (for example yearly) be replaced. There does not need to be a hard expiration limit however, a timestamp when the keys have last been replaces should suffice to indicate a key renewal should take place. It is advisable - but not necessary - to replace all 4 keys at once. The operation should not take a long time, but temporary locking the namespace to prevent simultaneous updates might be advisable. Only the record metadata and the public namespace directory records will need to be updated with symmetric encryption. Afterwards the symmetric keys need to be encrypted with the asymmetric public keys of the agencies and users with access to the namespace. The asymmetric operation will likely be more computationally intensive unless there are a huge amount of records in the namespace.

The record file blobs do not need to be re-encrypted regularly, making this operation much more feasible both in bandwidth requirements and computationally. The record file blobs are encrypted with a separate unique record key. When a record key is compromised only one record can be decrypted and an attacker can gain no further knowledge, so the damage that can be done has been done. Record keys will also be replaced on write, allowing for adoption of stronger cryptographic algorithms and key strengths by the occasional updates that are performed on records.

When a user revokes access rights to another party the namespace keys will have to be renewed as well to prevent unauthorised access. The procedure is exactly the same as described above, minus one public key encryption operation. Without the new keys the other party can only access and/or decrypt data that was previously accessed already.

4.2.3 Namespaces

The concept of personal namespaces is an integral part of this system design. Each separate namespace forms a authorization boundary and has a separate access control list (ACL). For each namespace there is a single owner that can assign the rights of others to find, read, or write to the namespace. The root of all other namespaces is the one place where a trust anchor is required, but trough the principle of *"minimal trust"*, abuse of this trust is limited to cases that constitute such blatant fraud that are easily detectable by anyone using the system. Trusting the root trust anchor, but being able to verify trust by detecting potential abuse trough open accountability, is a practical implementation that embodies the statement *"trust but verify"*.

Public Directory of Namespaces

The namespaces can be found in the public directory. For each namespace the owner key ID and the home service URL are looked up here. An example of the data contained in this directory is visible in table 4.3. The trusted root owns the root namespace, and assigns identity officials that can perform first level namespace writes on behalf of the trusted root. Only when the user registers trough an authorized identity official and the users primary key is issued is this new user namespace created. The root of the user namespace is a delegation point with the user's primary key identifying him/her as the owner. Inside the global root namespace the delegation record is signed by the identity official. The user has full control over any further namespaces and records below their root namespace. This includes the home service defined in their root namespace of any namespace below that. The namespace record in the public directory has to be signed with the owner key to allow verification of the authenticity of the namespace and home service URL.

Namespace	Owner Key ID	Home Service URL
/	trusted root	government service
/user12345/	user12345	organization a
/user12345/tax service/	user12345	organization a
/user12345/probation/	user12345	organization b
/user12345/company987/	pseudo12345	organization b

TABLE 4.3: Exposed example of public namespace directory

The metadata of which namespaces are available and which home services a user subscribes to are privacy sensitive metadata and should not be visible to everyone, this is obvious from the (wrong) example in table 4.3. For this purpose the namespace lookup key is used to store the logical namespace name as an HMAC (using SHA256), and the signed home service URL encrypted with AES256. To allow the root namespace of any user to be found the trusted root only writes the first level of the namespace with the well known public namespace lookup key by definition. This well known lookup key could be defined as an empty string (`""`). The namespace HMAC of user12345 would then be calculated as: `HMAC("", "/user12345/")`[1].

By also using well known namespace lookup keys for some standard users namespaces it is possible to create special namespaces that can be publicly located for each user. An example of a useful special namespace that should be made available by all users and agencies is a message inbox to allow the secure transmission (and reception) of namespace keys when namespace access is granted to them. To make this inbox namespace writable to everyone the namespace keys should either be published or a set of well known namespace keys can be used here as well.

A schematic illustration of a lookup of a user namespace home service trough the public directory is shown in in figure 4.5. The lookup is performed by calculating the HMAC with the namespace lookup key (which is well known for the root namespace, and has to be shared bu the user first for deeper level namespaces) and performing a lookup in the public directory. The home service URL is verified with the owner key, the owner key is subsequently verified with the identity official key, and lastly the identity official key is verified with the PKIoverheid identity CA. After these steps

[1] `e26da405a660f73b403d1f549d7515ec67eec030ad02daf1143c69675bed26a6`

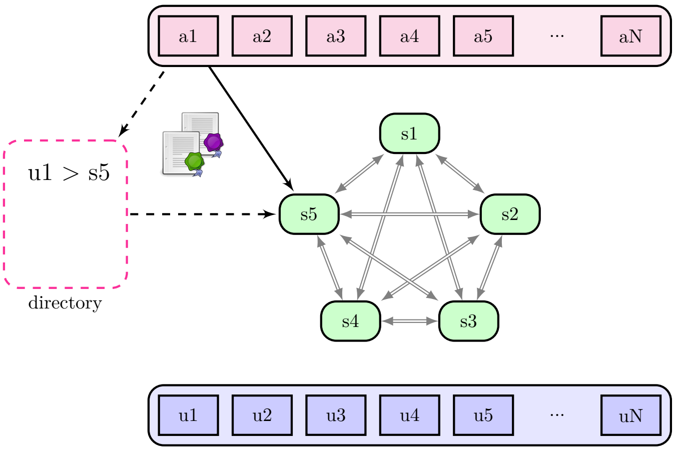


FIGURE 4.5: Agency a1 performs a lookup for a namespace of u1 by reading the public directory and verifying the signatures

the namespace home service can be contacted and the namespace queried. Depending on the keys that are available beside the namespace lookup key the access level is determined. Read operations can be performed when read access has been granted by sharing both the namespace metadata key and the namespace master key. Write access is subsequently granted by also sharing the namespace write key. Using these keys for writes to the namespace makes the written records available to all agencies and users that have been granted access to the namespace, as is illustrated in figure 4.6.

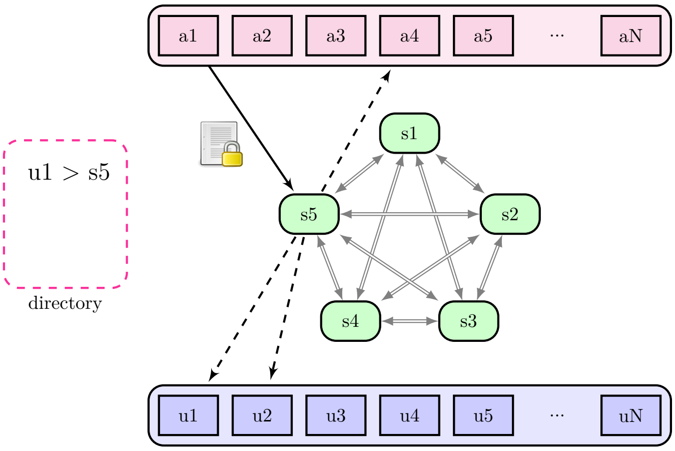


FIGURE 4.6: Agency a1 writes a record to the namespace of user u1 that is also shared by user with a3 and u2

Creating Namespaces

Creating a namespace will require the user to announce the namespace trough the public directory (after initialization of this namespace on the chosen home service). For this example we assume the user user12345 wishes to create a new namespace "duo" below their root namespace with the primary user key as owner key and the random namespace lookup key K_1. The following pseudocode shows the data written to the public directory:

```
Directory.Namespaces.Add(Sign(user12345,{
    "namespace":HMAC(K1,"/user12345/duo"),
    "owner_key":user12345,
    "home":Encrypt(K1,Sign(user12345,"Home URL"))
})
```

To allow someone to locate this namespace you need to share the namespace name ("/user12345/duo") and the namespace lookup key (K_1).

Namespace Owner Keys

A namespace can be created with any registered user key as the owner key. Theoretically a user can create all namespaces with the same identity provider primary key, however, this is generally not advisable. Beside the higher damage when losing the single primary key it is also a much larger operation to perform a key renewal operation as described on page 31. A better key management practice would be to create a separate subkey for each namespace and use this key as the namespace owner key. Additionally, the initial primary user key that is stored on the eID card should not be used as namespace owner key, but only to sign subkeys used as namespace keys. This seems similar to the Key Signing Keys (KSK) and Zone Signing Keys (ZSK) as mandated by DNSSEC [61]. However, in our system design this should not be a requirement, the choice to either use one key for all namespaces, or use separate subkeys at every delegation point should be left to the user and/or the software and hardware implementation they use. In practice this user choice is about a fundamental fundamental trade-off between the level of security, flexibility, and performance.

To facilitate easy key management of all subkeys (both for their main identity and their pseudonyms) users must be able to store these keys on their home service. Keys are encrypted with the public key of their primary key before storing them, when multiple primary keys are registered all keys should stored separately encrypted with each primary key. Additionally, users should be able to use an additional PIN or password per namespace subkey to provide an additional layer of security that can differ per namespace. The user can then authenticate with their eID card, download the encrypted subkeys for the namespace they wish to access, decrypt the subkeys with their private key, and optionally enter the additional password for the final subkey decryption step. The decrypted subkeys can subsequently be used to access all namespaces that offer the highest level of segmented security by using subkeys and are further protected by using an optional password.

Pseudonym Namespaces

A citizen has the right to have anonymous contact with many government services. It is thus necessary to be able to create namespaces under a pseudonym for this purpose. Creating the pseudonym key and namespace for "company" as listed in the example tables 4.1 and 4.3 above could have been performed with the following pseudocode:

```
pseudo12345 = GenerateKeypair()
linksig = LinkRegister.RequestSignature(
    Sign(user12345,pseudo12345.Public))
Directory.Keys.Add(Sign(pseudo12345,{
    "id":pseudo12345,
    "signature":linksig,
    "key":pseudo12345.Public
})
Directory.Namespace.Add(Sign(pseudo12345,{
    "namespace":HMAC(K2,"/user12345/company987/"),
    "owner_key":pseudo12345,
    "home":Encrypt(K2,Sign(pseudo12345,"Home URL"))
})
```

To protect the main identity the logical namespace name must not be shared with the agency, only the namespace HMAC. When you want to allow someone to locate the example pseudonym namespace with namespace lookup key K_2 you need to share the HMAC output (`HMAC(`K_2`,"/user12345/company987/")`) and the namespace lookup key (K_2). By appending a random code (in this example "987") to the namespace name the risk of the namespace name being recovered by brute force search is mitigated, protecting the main identity.

4.2.4 Record Storage

A record either consists of structured metadata, or a binary file with associated metadata. Metadata is stored on the home service to minimize metadata leakage from usage patterns and to have a trusted party maintaining the access logs. However, encrypted file blobs can be stored on any available online storage system. Because strong encryption with a random key is used the content of the file is secure. Furthermore, no identifying information should be stored with the file making it useless to an attacker that compromises the storage system.

Record Writing to Namespace

The basic steps to write a record to a user namespace are shown in the diagram in figure 4.7. In this diagram the home service stores the files on the storage service, but this could potentially also be reversed. When the agency stores the files on their own storage service only metadata is sent to the home service instead of all data. Changing the write order like this can offer a performance advantage at the cost of a higher risk of an incomplete write, when for example the agency incorrectly sends the metadata without waiting for the file transfer to the storage service to complete.

1. Prepare a signed request
2. Request home service location from directory
3. Return user home service location
4. Send request to the user home service
5. Authorise agency key + Log actions
6. Return OK + Encrypted namespace keys
7. Encrypt file blob(s) + metadata

8. Send file blobs + metadata
9. Verify write HMAC + Log actions
10. Forward file blob(s) to storage service
11. Report OK status to home service
12. Forward OK status to agency

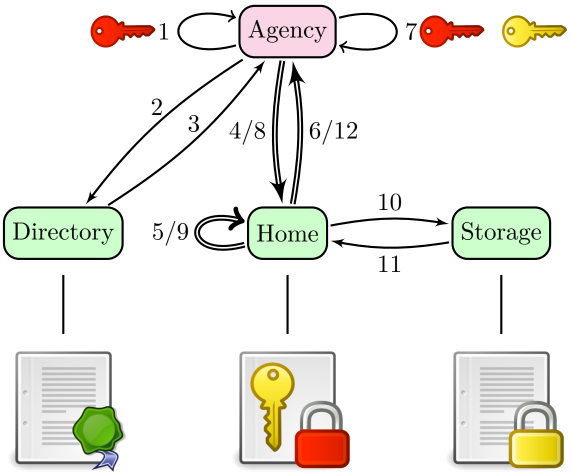


Figure 4.7: A schematic representation of the steps required to write a record to a namespace

Record Request from Namespace

The basic steps to request a record from a user namespace are shown in the diagram in figure 4.8. Steps 1 and 2 could be skipped if a previous record has been retrieved during this session, because the users namespace home service is known to the client at this point.

1. Request home service location from directory
2. Return user home service location
3. Prepare signed request
4. Send request to the user home service
5. Authorise user key + Log
6. Return encrypted metadata + encrypted keys
7. Client decodes metadata
8. Request file blob(s) from storage service
9. Return file blob(s) to client
10. Client decodes file blobs

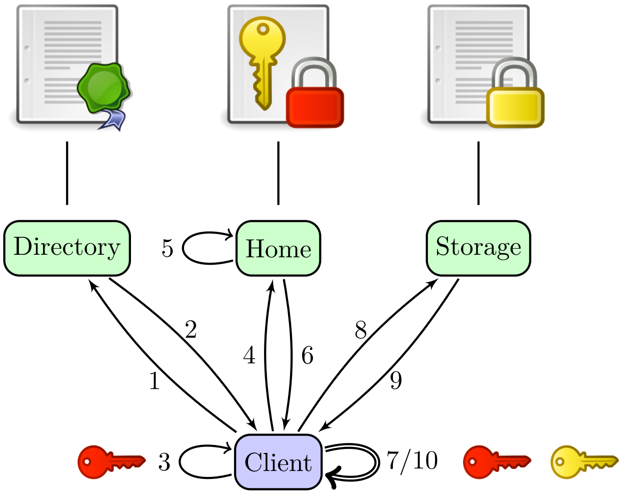


Figure 4.8: A schematic representation of the steps required to request a record from a namespace

Record Encryption

Encryption of a record consists of both the metadata encryption, and the file blob encryption. The following steps are executed to perform the encryption of a record:

1. Generate a random record key + random IV
2. Symmetrically encrypt the file blob(s) with the record key + IV
3. Store the encrypted file blob(s) on storage service and get URL
4. Symmetrically encrypt the record key with the namespace master record key + IV
5. Generate metadata including URL + the encrypted record key + IV
6. Sign the metadata with your private key
7. Symmetrically encrypt the file metadata with the namespace metadata key + IV
8. Generate an HMAC of the metadata with the namespace write key
9. Send the encrypted metadata + HMAC to the home service
10. The personal home service verifies the HMAC and signature and stores the metadata in the namespace

A simplified diagram with the keys that are involved is displayed schematically in figure 4.9. Also note that while the general process is the same as the process outlined in figure 4.7 some steps (such as writing to the storage service) have been changed in order to illustrate the procedure where the agency writes the file to their storage service, offering better performance.

An advantage of this encryption scheme is that a generic file (such as for example accompanying documentation that is sent as an appendix with

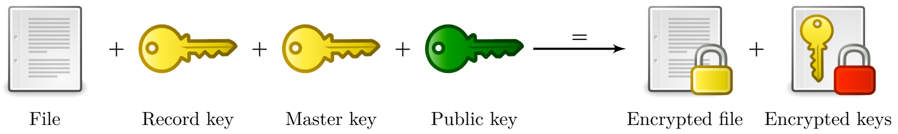


FIGURE 4.9: A file blob is encrypted with a random record key, which is encrypted with the namespace master record key, which is encrypted with a public key

another personalized record) that is sent to multiple users by an agency only has to be encrypted and stored once, allowing for some level of deduplication of generic data. The same IV is then reused for the metadata that is written to all receiving namespaces, but this should not pose a security risk since the namespace keys are different for each namespace. Because of this a user can also easily create a copy of (part of) a namespace with an entirely different ACL without having to re-encrypt the files. Copies of all namespace records the user wishes to copy are created by re-encrypting the record metadata with the keys of the new namespace, and storing these in the new namespace.

Record Decryption

Decryption of a record consists of both the metadata decryption, and the file blob decryption. The following steps are executed to perform a record decryption:

1. Decode the namespace keys with your private key
2. Validate the signature under the metadata to check signee
3. Decode the metadata of the record with the master record key + IV
4. Download the file blob(s) from the storage service URL
5. Decode the encrypted record key with the master record key + IV
6. Decode the file blob(s) with the record key + IV

A simplified diagram with the keys that are involved is displayed schematically in figure 4.10.

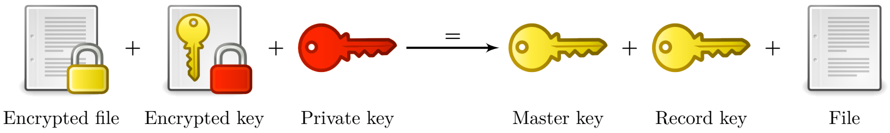


FIGURE 4.10: The encrypted file blob is decrypted with the record key, which is decrypted with the namespace master record key, which is decrypted with a private key

4.2.5 Failure Modes

Compromise of a Master System Key

If a master system key that is used to sign identity official certificates (the PKIoverheid root CA key used for eIDs) is compromised, all individual identity official certificates that are authorised to sign user keys must be re-signed with the new key. Recovery from this compromise requires the creation of a new root CA key for the chain of trust and is thus the worst key that could be compromised. The damage an attacker can do is limited by the fact that an attacker can only issue new falsified identity official keys and use these to initiate a user key re-issuance procedure (just like when the users key was lost). This attack is detectable by the user, the government, and any other party monitoring the public directory, so would not go by unnoticed. Additionally, these fraudulent re-issuance procedures could be rolled back so it would only cause a temporary denial of service. A compromised key does not require all user keys to be replaced or allow unauthorized data access to existing data. By introducing the re-issuance freeze period where no new data will be sent to the user after the notification of re-issuance we guarantee that an attacker will not receive any data at the fraudulently created new namespaces.

Compromise of a Server Key

The server keys are standard SSL certificates. If a certificate (or the PKIoverheid root CA for SSL certificates) is compromised, traffic going to the server could be intercepted with a man in the middle (MITM) attack. The data that is being send/received to the server is all encrypted, even inside the HTTPS stream. Only metadata about relations and usage patterns should be leaked to an attacker. When the compromised key is discovered the key should be revoked using standard PKI infrastructure means and a new certificate should be issued. All should should implement OCSP to check if the server key has been revoked.

Compromise of an Identity Official Key

If an identity official key that is used to sign user certificates is compromised, all individual user keys that are signed by that particular identity official will need to be re-signed. Because existing keys are only certified by the identity official and can not be issued at will there is no need to revoke all keys signed by the identity official key. To limit the impact for users, a identity official key should have a finite active life (ending long before expiration) and limit on the amount of signatures that are allowed with one key, and strict key security rules should be enforced (there is no reason for the key to ever leave the government building, or for the key to be recoverable from the smart card). The end of active life that is proposed to mitigate the impact of an identity official key is described on page 33. Additionally, the fraudulent re-issuance procedures could be started just like described in the case of the compromise of a master system key on page 42.

Compromise of User Key

If (or perhaps when, given the volume of user keys this system will contain) a user key is compromised, an attacker can gain access to (part of) the user namespace. The amount of data that can be accessed depends on the type of key. The worst case scenario would be a user that loses their their primary key that was used as the owner key all namespaces, resulting in all private data in that users namespaces to be accessible by an attacker. If, however, a namespace subkey was compromised, only the data contained in that namespace is compromised. Also in a case when the primary key is compromised, not all data from all namespaces will necessarily be compromised. If the user followed recommendation and protected individual namespaces with an extra PIN or password. In this case the primary user key can not decrypt the subkeys needed to access these namespaces. To protect against unauthorised access even when the primary key is lost it should thus always be recommended to the user to use subkeys for their namespaces and to additionally password protect the namespaces, especially the ones with the most privacy sensitive data. The revocation process of a user key is described on page 32.

4.3 Discussion of Proposed Design

We have proposed a design that uses familiar social constructs that can aid usability even though it has a high underlying technical complexity. All procedures, concepts, and security measures should be accessible and comprehensible to the average person (for example; picking up the eID smart card "key" in person, using an additional password for authentication, choosing where your namespace "digital vault" home server is located, giving explicit permission to agencies to access a namespace, and optionally adding an extra passwords to the namespaces with more privacy sensitive information). The proposed system can simultaneously offer privacy and security by design while being able to meet all government requirements.

The strong cryptography and other technology used in the design has been proven in practice. The technical part of the design proposal is an exploratory possible combination of these technologies aiming mainly to provide a technological basis for a discussion of transparency enhancing technology. This theoretical technical design seems feasible in theory, but it's strengths and weaknesses will only emerge after further exploration, discussion, and testing of a practical implementation. In general the practical success of a design depends strongly on the implementation that follows it. As with the initial design process the principles of privacy and security by design should be applied to the next steps in the process.

Chapter 5

Conclusions

A strong transparency enhancing system that protects citizens privacy seems vital to a well functioning participatory democracy. Gaining the peoples trust is a very important Dutch political goal which hinges both on public perception and the technical quality of the system. Historically, the security of important Dutch digital services have not always been of exemplary quality. The Netherlands currently is a few steps behind neighboring countries in the development of strong authentication. Catching up, and even exceeding the capabilities of other countries can thus also be seen as a matter of national and political prestige. Creating a transparency enhancing system that offers citizens transparency, privacy, security, control, and a user-centric experience, is a prestigious goal worthy of international acclaim.

We have found that existing technical solutions do not provide the transparency, privacy, and security required to promote strong trust and confidence in such a system. Although the latest standards and technology that are currently being developed are significant steps in the right direction, a combination of all the currently available Dutch technologies however still falls short of the ambitious government goals. A new system that does provide the transparency and control over personal data, as is mandated by Dutch law and regulations, will still have to be developed.

Our proposed design outlines a potential solution to our research question. Advantages of this design are the socially familiar procedures, conformity to existing identity provider frameworks, choice of identity- and private home service providers, flexibility of namespaces for granting fine-grained access rights, reliable service scalability, technological feasibility, minimal verifiable trust needed, and private and secure by design. Potential disadvantages of this system could consist of the inherent requirement for trust - albeit minimal - in a multitude of parties, integration issues in a heterogeneous network, implementation shortcomings due to the complexity of the design, and potential security weaknesses due to the still unproven design.

During this research project we have shown that transparency enhancing technology that does not negatively impact user privacy is feasible. Not only is this feasible, but a design that offers transparency, privacy and security will most likely be essential to the success of the system. Upholding these values is important to the public opinion, as is conformity to familiar social experiences. When transparency, privacy and security are being offered to people in a user friendly manner the design will more easily be appropriated by the people.

The theoretical basis provided by our proposed system design satisfies the government requirements, and provides privacy and security by design. When our design is further developed trough an open design process that adheres to privacy and security by design principles from start to finish, a trustworthy system could be offered for use by citizens, businesses and government agencies of the Netherlands. Support from these different parts of society will all be equally important to the social as well as the political success of the system.

We believe reports such as this can help contribute to a broader discussion aimed to achieve a good practical transparency enhancing system design, and aid the promotion of stronger social and political support for such a system. Visibility and transparency of the system design process seem essential prerequisites to establish trust and accountability, and the open nature of academic research helps instill these and establish a well founded design process. Transparency enhancing technology for use by the government that does not negatively impact citizen privacy is possible trough an open process based on academic research and founded on the principles of *"privacy and security by design"*.

Chapter 6

Recommendations

The following list of action-oriented recommendations are made to the Dutch government, and other parties related to the design and development process of transparency enhancing technology in the Netherlands. These recommendations should generally be feasible, and are in line with the government's plans for a digital government in the future.

1. The Dutch government should keep their current course with a stronger demand for an open design process for future transparency enhancing technology, and the infrastructure components that support it, such as identity providers. Transparency of the design is required for *"privacy and security by design"*, and demanding this should promote trust and confidence in the design process, as well as the future system implementation.

2. Technological design documentation for privacy crucial infrastructure should be published before any implementation. A proactively open and transparent design process is crucial to develop a system that is secure and private by design. No/late publishing of technological design choices will likely lead to less early scrutiny and a reactive approach to security and privacy after implementation.

3. STORK 4 strong authentication mechanisms based on smart card technology should be made available to all citizens in the Netherlands. STORK 3 authentication should only be used as a stopgap measure, and the strength of cryptography should be upgraded when possible (use STORK 3 means of authentication with STORK 4 strength cryptographic implementation).

4. Provide additional accountability by identifying and registering (the signature of) the issuer of STORK 4 tokens personally. This helps combat fraud, and increases social confidence because the digital trust model closely mimics the social trust model.

5. Legal prosecution of digital identity fraud should be aggressively enforced with personal liability for identity officials in the case of negligence, and fines and/or other legal repercussions against identity providers in the case of failure to comply to security procedures leading to key compromise.

6. PKIoverheid should implement a sub CA with separate procedures to facilitate frequent renewal of identity official certificates, allowing keys with an early end of life to be used, which mitigates impact when an individual key is compromised.

7. Digidentity should create an update for their Digidentity app that does not store key data unencrypted in an SQLite database but utilizes the key store for added security. Additional checks if device is rooted to warn the user against storing private keys on an insecure device are also recommended.

8. Digital Me should create an update for their Dappre app that does not store personal data unencrypted in an SQLite database but utilizes the key store to store for added security. Additional checks if device is rooted to warn the user against storing personal data on an insecure device are also recommended. A third recommended change is to disallow the e-mailing of the QR code to link to your profile, which is a convenient security risk because the secret used to set up the secure link can be intercepted by an attacker.

9. The Netherlands should lobby for a European research grant specifically to develop technology that allows ubiquitous securely access to (STORK) smart cards from web based services. This grant could for example be divided between the W3C for further development of the Web Cryptography API, and open source browser developers such as Mozilla.

10. The Forum Standardization should publish an expert recommendation about cryptographic standards and principles that must be applied for personal authentication/signing/decryption (for example for use with eID / Idensys). This must lead to a regular (for example annual) update with an updated roadmap that includes dates when new technology should be implemented and deprecated technology will no longer be supported.

Chapter 7

Discussion

7.1 Ethical Issues

For this project we did not expect any ethical issues. Our proposed design does not have any immediate ethical issues. When deployed as a practical implementation there may be ethical consequences, both positive and negative as is always the case with technology. The future ethical consequences will be based on the specific technical implementation, associated procedures and the political-social context of governance.

However, during our research into existing Dutch technology we did raise some ethical issues. We have identified a major security issue in the Digidentity app that can potentially be exploited to circumvent 2FA for eID / Idensys that is used to access government services. When this security issue can be exploited in the wild the practical authentication security level will be significantly lower for all government services, health care providers, and other companies that are accessible by this means of authentication[1]. This issue has been reported to the OS3 ethical commission and a responsible disclosure procedure will be started.

Additionally, we found a minor privacy issue in the Dappre app that can potentially be exploited to gain personal data of the user and other people that linked with their Dappre app. This issue does not pose a significant security risk, but because of the user expectation of privacy that is not being offered by the app this certainly is an ethical issue. This issue has also been reported to the OS3 ethical commission and a responsible disclosure procedure will be started.

7.2 Future Work

This report consisted of a broad design exploration. Much further research into many facets of transparency enhancing systems can be performed. The potentials for systems that offer transparency, privacy and security are practically limitless. These are some of the potential avenues for further research:

1. Perform further research into system architecture designs that combine transparency, privacy and security.
2. Create a proof of concept implementation for a federated transparency enhancing system for real-world testing.

[1] https://www.idensys.nl/inloggen-met-idensys/over-de-testen/

3. Work on practical browser technology to universally support online smart card technology on all systems.
4. Perform a more thorough security examination of the eID / Idensys implementations (currently only Digidentity).
5. Perform a more thorough security examination of the Qiy framework implementations (currently only Dappre).
6. Perform security exploration into risks of a single form of authentication for government, health care and business.
7. Perform research into using designs similar to the proposed system design for health care medical data record sharing.
8. Perform research into using designs similar to the proposed system design for secure message passing for an e-mail 2.0 application.
9. Perform research into e-voting technology, specifically if and how existing eID technology could be used to facilitate e-voting.
10. Perform research into post-quantum cryptography to replace existing cryptographic algorithms in the design.

7.3 Personal View

Firstly, I applaud the strong government initiative to provide citizens with transparency and control over their data. Commitment to granting citizens these personal rights shows true visionary leadership. Secondly, I fervently support the right to personal privacy, and I believe that technology can be used to protect privacy if we are vigilantly pursuing it at every step of a new design. Thirdly, security is a requirement for privacy that goes hand in hand with it, and in my opinion you can never have one without the other. During this project these three values of transparency, privacy, and security have been combined in search of a balanced solution. I hope my personal contributions have helped solidify the fact that transparency, privacy, and security are not mutually exclusive, and promote the idea that these are ideals we need to strive for. We should not settle for a solution that fails to deliver on one of these important values. If this report has managed to convince you - the reader - that these values are attainable, I feel I have succeeded in my humble mission to promote these values.

Appendices

Organization	**Directly involved or via group**
Agentschap NL	Both directly and in Manifestgroep
Belastingdienst	Both directly and in Manifestgroep
CAK	Via Manifestgroep
CBS	Via Manifestgroep
CIZ	Via Manifestgroep
CJIB	Via Manifestgroep
CVZ	Via Manifestgroep
Dienst Regelingen	Via Manifestgroep
Divosa	Directly
DUO	Both directly and in Manifestgroep
Forum Standaardisatie	Directly
Informatie Management Groep	Directly
Inspectieraad	Via Forum Standaardisatie
Iterprovinciaal Overleg	Via Forum Standaardisatie
IND	Via Manifestgroep
Kadaster	Via Manifestgroep
Kamer van Koophandel	Via Manifestgroep
King	Directly
Logius	Directly
Manifestgroep	Both directly and via Forum Standaardisatie
Ministerie van Veiliheid en Justitie	Both directly and via Forum Standaardisatie
Ministerie van BZK	Both directly and via Forum Standaardisatie
Ministerie van Financiën	Both directly and via Forum Standaardisatie
Ministerie van EZ	Both directly and via Forum Standaardisatie
Ministerie (other)	Via Forum Standaardisatie
NVVB	Directly
RDW	Via Manifestgroep
Social Impact	Directly
SVB	Both directly and in Manifestgroep
Top- kring Dienstverlening Gemeenten	Directly
UWV	Both directly and in Manifestgroep
UVW	Via Forum Standaardisatie
VDP-leden	Directly
VGS	Directly
VIAG	Directly
VNG	Both directly and via Forum Standaardisatie

2001 ICTU[1] is established to work on a digital government.

2002 The first initiave is taken for a digital customer file or vault, the first data added to Suwinet was UWV.

2003 The Manifestgroup is established[2]. The first version of DigiD was created (then named '*Burgerpin*').

2004 The SVB took initiative with the '*Burgerpolis*'[3], a fairly abstract idea of the future of how government should interact with citizens in a digital world, and respecting the rights of citizens.

2005 Starting this year all online government services use DigiD for authentication. The commissie Keller researched the digital services of CWI, which resulted in the term "*Digitaal Klantdossier*".

2006 Logius is formed (first named '*GBO.Overheid*'[4]) to develop generic ICT infrastructure. The Forum Standardisation[5] is also established to develop and establish electronic standards for communication.

2007 The government specified the need for Open Standards and Open Source to help provide Supplier- Independence, Interoperability, Transparency, Checkability and Manageability and Digital sustainability [72].

2008 The government starts i-NUP, the national government implementation programme for services and e-government [5].

2009 SVB takes renewed initiative with the '*Burgerpolis*' [73]. The first steps to '*SUWIweb*' are also made. This year the '*Wet eenmalige uitvraag'* was enacted, which amongst others enforces the data sharing of personal data so citizens only have to provide this once for all the agencies concerned with work and income. This year the first test version of MijnOverheid also goes live.

2010 The VNG took initiative to put service to citizens first. Dutch cities cooperate more to exchange data securely. eHerkenning[6] goes live and starts providing secure authentication to government services for business.

2011 The Manifestgroup published their envisioned digital future. Logius takes control of MijnOverheid and other government services. i-NUP publishes the status of the programme [6].

2013 Minister Plasterk officially released his vision of a digital future, and with a target set to realize this by 2017 [1]. Work is begun on changes in law to solidify the legal basis for this vision. The government also

[1] https://www.ictu.nl/over-ictu/

[2] https://manifestgroep.pleio.nl/manifestgroep

[3] https://www.doorneweerd.nl/politiek/burgerpolis

[4] https://www.logius.nl/over-logius/jaaroverzichten/jaaroverzicht-2009/over-logius/

[5] https://www.forumstandaardisatie.nl/english/

[6] https://www.eherkenning.nl/en/over-eherkenning/ontwikkelingen/

released the report '*de burger bediend*', a report on the (in)secure use of Suwinet [74]. The specification for the new eID stelsel that will replace DigiD and eHerkenning was finished.

2014 The Manifestgroep together with multiple other (government) agencies release their vision for the digital future in 2020 [2]. The forum standardization publishes their latest version of the practical requirements on authentication [26]. MijnOverheid is now also part of the tools offered by the Forum Standaardisatie. i-NUP programme is officialy concluded, but continues in other forms.

2015 Logius specifies the latest MijnOverheid practical requirements which reflect earlier future visions. The 2017 government wide implementation agenda for digital services is released by the council of governments [10]. The final report of the i-NUP programme is released [7], the minister summarizes the final report and concludes work needs to continue and tasks the '*Nationaal Commissaris Digitale Overheid*' with this [75].

2016 MijnOverheid reaches 3 million users[7]. This year the European standard guidelines for online government services should be accepted. The Dutch law regarding GDI should also be finalized [24].

[7] `https://www.rijksoverheid.nl/actueel/nieuws/2016/01/25/drie-miljoen-mensen-activeren-berichtenbox`

The following requirements are based on various documents released by the Dutch government. The relevant parts of references are quoted and our interpretation is clarified.

1. ***Users (citizens) have a right to know what data is stored by various (government) agencies***

   (i) *"Inzage- en correctierecht voor burgers [. . .] Burgers moeten eenvoudig kunnen zien welke gegevens over hen zijn vastgelegd en aan wie deze worden verstrekt."* [1, p.5] Also an intermediate step towards this goal that is mentioned is '*MijnOverheid*', which we have described in more detail on page 12. Note that the right to transparency of personal data is already written in law.

   (ii) *"De SVB onderschrijft het belang van inzagerecht, correctierecht en transparante verwerking van persoonsgegevens voor de burgers en geeft hier ook prioriteit aan, getuige de leidende rol van de SVB in het uitdragen van de Burgerpolis als dienstverleningsconcept. Uitgangspunten van de Burgerpolis zijn:*
   De burger krijgt inzage in zijn bij de overheid opgeslagen gegevens;
   De burger heeft de mogelijkheid om foutieve gegevens te corrigeren;
   De burger wordt persoonlijk benaderd en ontvangt informatie die persoonsgebonden is;
   De burger wordt actief geïnformeerd en tweerichtingsverkeer is mogelijk." [74, p.29]
   The '*Burgerpolis*' is the way The Sociale Verzekeringsbank (SVB) envisions data exchange with citizens in the 2020 goal.

   (iii) *"Een eerste stap is het aansluiten van meer overheidsinstanties op mijnoverheid.nl. Uiteindelij k is het doel niet één overheidsloket, laat staan één allesbevattende website of bestand. Het doel is een voor iedereen toegankelijk recht op zekerheid."* [73, p.7] Connections of more government organizations to MijnOverheid is a first step towards sharing data on citizens, and finally to integrate in the future single government '*Overheidsloket*'. This goal is now being worked on by the Manifestgroep and Logius.

   (iv) *"De burger is regisseur van zijn eigen informatie. Dit is geen utopiedenken. Al door de invoering van een digitale kluis kunnen burgers en bedrijven inzien welke gegevens er bekend zijn, bepalen wie toegang heeft."* [76, p.17] Citizens and businesses have a right to see what data is stored about them. The system is described here as a 'digital vault'.

   (v) *"Als klant hoef ik gegevens maar één keer aan te leveren en kan ik gebruik maken van proactieve diensten. Der overheidsorganisaties maken inzichtelijk wat zij van mij weten en gebruiken mijn gegevens niet zonder mijn toestemming."* [77, p.26] [11, p.42] The 'customer' of government services only has to share data once, can see what data government agencies have stored about them, and has to give permission for use of this data.

2. ***Users should only have to provide their data to the government in one place***

(vi) *"Diensten en informatie worden hiervoor beschikbaar gemaakt via een centraal (knoop)punt. Burgers worden niet lastig gevallen met de verschillen tussen publieke organisaties: ze hebben te maken met één overheid."* [1, p.7] Government services should be available trough one central system giving users the convenience of dealing with one government.

(vii) *"Daarnaast wordt in dat kader de mogelijkheid onderzocht om de burger een recht te geven op het slechts eenmalig hoeven aanleveren van gegevens aan organisaties van de Rijksoverheid."* [2, p.13] It is being reseached if it is possible to give citizens the right to only have to share their data with the government once.

(viii) *"Op langere termijn is de intentie dat de burger zijn gegevens daadwerkelijk maar één keer hoeft te verstrekken aan de overheid. We zouden dan kunnen spreken van een 'weigeringsrecht': de burger of het bedrijf mag dan weigeren om zijn gegevens aan een overheidsinstantie aan te leveren als hij mag aannemen dat deze gegevens bij de overheid bekend zijn. Dat laatste leidt voor de burger of het bedrijf direct tot administratieve lastenverlichting."* [5, p.25] Citizens should have a 'refusal right' to prevent having to give their data to a government agency when the government already has this data.

(ix) See reference (v)

3. ***A system to which both users and agencies connect is needed to facilitate this***

(x) *"Gemeentelijke organisaties zullen geholpen worden door het Kenniscentrum Dienstverlening om het gebruikersperspectief een meer centrale plaats te geven in het dienstverleningsproces. Dit samenwerkingsverband tussen BZK, VNG en KING adviseert gemeenten bij het betrekken van gebruikers bij het ontwikkelen van (digitale) diensten op een pragmatische manier, waarbij verbeteren van processen continue mogelijk is en wordt gestimuleerd. Het ontbureaucratiseren van processen bevordert niet alleen een snellere en betere dienstverlening, maar is ook een belangrijke voorwaarde voor een gebruikersvriendelijke digitalisering."* [1, p.4]

(xi) *"Een belangrijke stap daartoe is om burgers via MijnOverheid inzage te geven in de kerngegevens die overheden over hen vastleggen, met de mogelijkheid om online correcties door te geven. Hiermee wordt verder invulling gegeven aan het inzage- en correctierecht uit de Wet bescherming persoonsgegevens."* [1, p.5]

(xii) *"Het is belangrijk dat we met elkaar verder bouwen aan wat er al loopt op het terrein van de basisinfrastructuur. Afspraken uit het iNUP worden uitgevoerd en waar mogelijk versneld. Burgers verwachten één overheid en daarbij hoort eenduidigheid en hergebruik van generieke voorzieningen. Bovendien bevordert een generieke basisinfrastructuur veiligheid en stabiliteit in ketens. Tenslotte is hergebruik van een generieke basisinfrastructuur goedkoper."* [1, p.7] New systems must build on existing government basis infrastructure. Reuse of this infrastructure helps promote safety, stability and is cheaper. The iNUP is the national government implementation programme for services and e-government outlined in 2008 [5].

(xiii) *"Diginetwerk is het besloten netwerk van de overheid. Via Diginetwerk kunnen overheden gegevens die een hoge mate van beveiliging vereisen, veilig uitwisselen met andere overheden. O.a. Haagse Rink, Suwinet en GEMNET zijn onderdeel van Diginetwerk."* [78] A government network ('*Diginetwerk*') connecting government services such as Suwinet (which is used for personal data exchange between local city governments) already exists.

(xiv) *"Diensten en informatie worden hiervoor beschikbaar gemaakt via een centraal (knoop)punt. [. . .] Dit betekent dat in 2020 alle digitale dienstverlening van overheden via de overheidspoort ontsloten wordt."* [2, p.13]

(xv) See reference (iii)

4. ***Users must be able to authenticate securely with a strong personal identification mechanism***

(xvi) *"[. . .] nieuwe technologische ontwikkelingen en de noodzaak van betere beveiliging moeten we vooruitkijken naar een zwaardere vorm van authenticatie dan DigiD."* [1, p.6] We more secure authentication than DigiD, and are in fact moving to the eID system for this purpose.

(xvii) *"Vaststellen van de identiteit van een partij (authenticatie)" + "Bewijzen dat je bevoegd bent om bepaalde diensten en producten af te nemen (autorisatie)" + "Het kabinet is uitdrukkelijk van mening dat er voluit ruimte moet zijn voor inzet van private eID-voorzieningen, ook voor natuurlijke personen."* [34, p.3-4] In practice this will result in commerical smart cards which will offer '*STORK 4*' level authentication which is described in page 9. The documentation further references the '*Forum Standaardisatie*' for more details, which is elaborated on in page 1.

(xviii) *"Het publieke eID middel is te gebruiken voor authenticatie op een hoog betrouwbaarheidsniveau door burgers voor BSN-gerelateerde diensten, bijvoorbeeld het doen van aangifte voor de inkomstenbelasting."* [79, p.2] The eID system will be used with strong authentication for government services requiring BSN.

(xix) *"Private eID-deelnemers; Partijen die ervoor zorgen dat de authenticatie en autorisatie diensten voor burgers en bedrijven beschikbaar komen: hoogwaardige authenticatiemiddelen, gevalideerde attributen, machtigingsregisters en eID-makelaars."* [29, p.26] Private businesses will produce means of authentication, and also function as authentication providers.

5. ***Multiple strong authentication mechanisms must be supported, specifically international alternatives***

(xx) *"Momenteel wordt een concept Verordening elektronische identiteiten en vertrouwensdiensten besproken tussen de lidstaten van* *de Europese Unie. Deze verordening gaat onder andere de wederzijdse erkenning van identificatiemiddelen tussen de lidstaten regelen. Hierdoor wordt grensoverschrijdende elektronische overheidsdienstverlening aan burgers en ondernemers vergemakkelijkt. De verordening betekent dat Nederland middelen uit andere lidstaten, die vergelijkbaar zijn met de DigiD-kaart, moet kunnen accepteren."* [34, p.4] European regulation for cross-border digital means of identification is being worked on. The Netherlands must accept identification means similar to the '*DigiD-kaart*' (a now cancelled smart card based ID).

(xxi) *"Daarbij hebben we niet alleen met de Nederlandse markt te maken. Er is steeds vaker sprake van grensoverschrijdende dienstverlening, waarbij ook met buitenlandse authenticatiemiddelen toegang moet kunnen worden verkregen tot Nederlandse diensten."* [26, p.20] Services are more and more cross-border, and foreign means of authentication need to be accepted for access to Dutch services.

(xxii) *"Door uitvoering van de Europese projecten STORK en STORK 2.0 is er ervaring opgebouwd om grensoverschrijdende authenticatie in Europa mogelijk te maken. Nederland is ook deelnemer aan het STORK project. Binnen STORK wordt een infrastructuur beproefd om een gebruiker digitaal toegang te geven tot buitenlandse dienstaanbieders na authenticatie met zijn eigen nationale eID. Een goede technische en organisatorische aansluiting van het eID Stelsel NL op de beproefde infrastructuur is op termijn noodzakelijk om de ontsluiting van middelen uit andere EU-landen te kunnen faciliteren."* [79, p.3] The Netherlands participates in the STORK project and will thus have to adapt their existing infrastructure to support STORK authentication means. With STORK authentication a user can also use online government services with the authentication from another European country (see page 9).

(xxiii) *"De in april 2014 aangenomen Verordening elektronische identiteiten en vertrouwensdiensten stelt eisen aan het eID Stelsel NL. Binnen het Europese integratieproject wordt gewerkt aan één interne digitale markt door de realisatie van internationale, grensoverschrijdende, eOverheid toepassingen die de administratieve lasten voor burgers en bedrijven verlagen en de Europese integratie bevorderen. Een voorbeeld hiervan is het STORK project waar een infrastructuur ontwikkeld wordt voor grensoverschrijdende authenticatie."* [29, p.34] Within Europe one market for digital services is being realized. An example is the STORK European framework for strong authentication (see page 9).

6. *Agencies can securely and verifiably enter, modify and read (a subset of) data stored on a user*

(xxiv) *"Bij retourberichten is het belangrijk dat de dienstaanbieder de volgende zaken goed regelt: Het bericht of document moet de geadresseerde bereiken; Onbevoegde derden moeten geen toegang kunnen krijgen tot het bericht of het document; De geadresseerde moet kunnen verifiëren dat het bericht of document ook daadwerkelijk* *afomstig is van de betreffende dienstaanbieder."* [26, p.41] The message sent by the agency must securly and verifyably arrive at the user and must not be able to be read by any unauthorised third party.

(xxv) *"Dienstaanbieders kunnen retourberichten op een eigen webportaal zeten en burgers daar dan toegang toe geven met bijvoorbeeld hun DigiD. Zij maken echter steeds vaker gebruik van de generieke voorziening Berichtenbox (onderdeel van MijnOverheid) in plaats van hun eigen webportaal. In de Berichtenbox kunnen de geadresseerden (retour)berichten van de overheid openen en lezen in een veilige omgeving. [. . .] Ervan uitgaand dat de omgeving van de Berichtenbox (c.q. het webportaal zelf) voldoende beveiligd is, blijkt het belangrijk er zekerheid over te hebben dat de juiste persoon toegang krijgt tot de betreffende berichten. Daartoe biedt de Berichtenbox voor burgers zekerheden tot betrouwbaarheidsniveau 2 door toegang te verlenen met DigiD en aan de hand van het verkregen BSN de toegang tot de berichten van een persoon te beperken. Dat een document afomstig is van de overheid weet de geadresseerde vrij zeker, aangezien de bron de Berichtenbox of een andere vertrouwde webdienst is."* [26, p.43] Agencies can send messages to a user via the MijnOverheid messagebox (see page 12). Trough the use of this secure service both the agency and the user trust MijnOverheid (trough identity provider DigiD) to verify the other parties identity.

(xxvi) *"Zowel de burger als de overheidsorganisatie moeten kenbaar maken dat de elektronische weg openstaat. Wat betreft kenbaarmaking door de burger moet 'voldoende betrouwbare' informatie beschikbaar zijn over het elektronische adres waar hij bereikbaar is. Opties die daaraan voldoen zijn: Registreren op een portaal waarop informatie voor hem kan worden klaargezet."* [26, p.83] The agency and the user must both make the option for online communication known.

(xxvii) *"Een organisatie kan alleen berichten versturen naar burgers die een actief MijnOverheid account hebben en zich hebben geabonneerd op berichten van de betreffende organisatie. Een organisatie moet dit vooraf controleren via de functies van Opvragen geabonneerden."* [78, p.7] An agency can only send a message to users that have registered a MijnOverheid account and have subscribed to that specific agency.

(xxviii) *"Het is van belang dat maatschappelijke organisaties niet zomaar toegang krijgen tot persoonlijke gegevens in de Burgerpolis, anders dan de gegevens die zij zelf beheren."* [73, p.10] It is important that agencies do not get access to personal data by default, other than the data they themselves manage.

(xxix) See reference (iv)

7. ***Users can view their data stored by agencies and enter and modify their own personal data***

(xxx) *"[. . .] Daarnaast moeten zij de mogelijkheid hebben om fouten te (laten) corrigeren."* [1, p.5] Users must have the possibility to perform (or request) correction of errors.

(xxxi) *"Burgers zijn zelf verantwoordelijk voor de juistheid van hun gegevens en kunnen hier binnen vastgestelde kaders zelf mutaties in doorvoeren."* [2, p.13] Citizens are responsible for the correctness of their data and can perform changes themselves.

(xxxii) *"Er zijn (technische) voorzieningen ten behoeve van correctlev-erzoeken gerealiseerd, zoals Suwinet-Correctie, Mijnoverheid.nl, DKD, en herstelfaciliteiten bij de vooringevulde aanvraagformulieren. Daarmee voldoen de uitvoeringsorganisaties aan de door de Inspectie gehanteerde norm. Er is ook voldoende draagvlak voor een correctiefaciliteit voor de burger en het belang daarvan wordt onderkend. Het gebruik van de geboden correctiefaciliteiten is echter nog beperkt. Dit hangt mede samen met het feit dat burgers niet (actief) worden geïnformeerd over correctiemogelijkheden en vaak niet duidelijk is wie fouten moet corrigeren. Hierdoor laat het wettelijk recht op correctie, dat is vastgelegd in de WBP, zich moeilijk effectueren. [. . .] Het feitelijk gebruikvan inzage- en correctievoorzieningen door burgers is beperkt, wat het beeld voedt dat de burger weinig behoefte zou hebben aan transparantie. Hierdoor onderschatten uitvoeringsorganisaties en gemeenten het belang van de burger. [. . .] De uitvoering biedt de burger correctievoorzieningen, maar deze worden nauwelijks door de burger gebruikt."* [74, p.20-21] The government noticed that the right to view and correct your own data saw limited use. The government first concludes that they do not communicate these possibilities to citizens, and it is not clear who can correct mistakes in data. The legal right of citizens was thus hard to be used in the past.

8. ***Users can give permissions to other users and agencies to access (a subset of) their data***

(xxxiii) *"Burgers bepalen zelf wie die gegevens mogen gebruiken."* [2, p.13] Citizens can decide themselves who can use their data.

(xxxiv) *"Burgers bepalen welke organisaties welke gegevens mogen inzien."* [34, p.10] Citizens decide which agencies can see their data.

(xxxv) *"Er komt één eID Stelsel voor authenticatie- en bevoegdheidsdiensten, te gebruiken bij elektronische transacties door natuurlijke en niet-natuurlijke personen waardoor: a. Dezelfde standaarden gelden voor het burger- en bedrijvendomein; [. . .]"* [26, p.6] There will be one eID system for authentication and authorisation. The same standards apply to citizens and business.

(xxxvi) *"Om vertegenwoordigingssituaties in de elektronische wereld beter te regelen, is het van belang te streven naar expliciet vastgelegde machtigingen. [. . .] Dit risico [op fraude] dient te worden ondervangen; ten eerste door iedere keer dat een dienst wordt afgenomen een machtiging te vereisen en ten tweede door voldoende stringente eisen te formuleren aan de registratie en het gebruik van machtigingen, via referentie aan normatieve documenten op dit* *gebied (van eHerkenning, of straks eID stelsel NL dan wel Europese voorschriften)."* [26, p.37] It is important to explicitly record permissions to allow others to represent you. To combat fraud this must be done with strict standards for registration and mandating others (with eHerkenning, the eID system, or European guidelines).

(xxxvii) See reference (xxvii)

9. ***Users can issue a mandate to another user to allow this user to manage their data***

(xxxviii) *"Het eID Stelsel beschrijft de werking van de volgende elektronische vertrouwensdiensten: authenticatie, het vaststellen van bevoegdheden om voor een ander te handelen (machtiging en wettelijke vertegenwoordiging), het leveren van attributen (zoals beroepsbevoegdheid of voldoen aan een leeftijdsgrens), en ondertekenen." [... "Hierin wordt op een betrouwbare wijze geregistreerd dat een persoon een andere persoon heeft gemachtigd namens hem/haar diensten af te nemen bij een dienstverlener. Het machtigingenregister voor natuurlijke personen kan zowel publiek als privaat worden aangeboden. Het machtigingenregister voor rechtspersonen wordt - mits aan bepaalde voorwaarden wordt voldaan – uitsluitend privaat aangeboden."* [34, p.6-7] The eID system provides authentication, permissions, attributes, and signing. When another user is mandated to use government services in their behalf it is securely registered. This register can be a public government service or a private business service.

(xxxix) *"De handelende persoon handelt niet voor zichzelf, maar is bevoegd vanwege de uitoefening van een erkende persoonsrol. De handelende persoon handelt niet voor zichzelf, maar is specifiek voor die belanghebbende bevoegd vanwege het bestaan van een wetelijke vertegenwoordiging (zoals bestuurders van rechtspersonen, eigenaren van eenmanszaken en curatoren) of vanwege een door de belanghebbende verstrekte volmacht (een privaatrechtelijke volmacht op basis van artikel 3:60 BW of een bestuursrechtelijke machtiging op basis van artikel 2:1 Awb)."* [26, p.87] There is a strong legal basis to issue a personal or legal mandate to manage your affairs written in Dutch law.

(xl) *"Artikel 5 Gebruik DigiD Machtigen 1. Een vertegenwoordigde of beoogd gemachtigde kan een aanvraag tot registratie van een machtiging doen via machtigen.digid.nl of via een afnemer die het aanvragen faciliteert. 2. De aanvraag en registratie van een machtiging kunnen betrekking hebben op een of meerdere diensten van een of meerdere afnemers en kennen een vooraf bepaalde geldigheidsduur. [...]"* [9, p.2-3] A person can authorise another user trough 'machtigingen.digid.nl'. This authorisation can be for one or more government services, for one or more people, and are only valid for a predetermined duration.

(xli) See references (xxvii), and (xxxiii)

10. ***Agencies can issue a mandate to other agencies/users (employees) to access data of users (citizens)***

(xlii) *"Een derde partij (intermediair) mag berichten namens een afnemer berichten afleveren bij MijnOVerheid. Mits deze organisatie met haar klant een bewerkersovereenkomst in relatie tot Logius als bewerker heeft getekend."* [78, p.7] An agency can let a third party handle messages when an agreement is signed to mandate this.

(xliii) *"Door intensieve samenwerking en informatiedeling tussen organisaties (overheden, ketenpartners en bedrijven) realiseren we administratieve lastenverlichting, besparingen en betere prestaties. Zowel in eenvoudige dienstverlening als complexe maatwerkdienstverlening. Vraag en opgaven staan centraal, niet de organisaties, instituties. Burgers en bedrijven begrijpen in 2020 wat de overheid over hen weet en wat met die kennis gebeurt, wet- en regelgeving kan daarmee drastisch vereenvoudigen. Hierdoor verdwijnen overbodige processtappen en handelingen, van overheid en burgers. [...] Om effectievere en efficiëntere dienstverlening te realiseren is een verandering van privacy wetgeving onvermijdelijk."* [2, p.15] Intensive cooperation and data sharing between agencies is needed for efficiency and cost savings. To realise this changes to the privacy law are needed.

(xliv) See reference (xxxiv)

(xlv) Implied by the social fact that data is finally processed by a natural person. This specific user needs access to the data on behalf of the agency and should be accountable for unauthorised access. Auditing also implies the user inherits the authorization of an agency, otherwise the audit logs are on the level of entire agencies, which does not provide the level of accountability needed to combat fraud and privacy violations.

11. ***Users can revoke permissions, including default permissions to agencies***

(xlvi) *"De registratie van een machtiging eindigt door het intrekken van de geregistreerde machtiging of na het verstrijken van de geldigheidsduur."* [9, p.3] Permissions end either by being revoked or after expiration of the predetermined duration.

(xlvii) See references (xxvii), (xxxiv), and (xl)

(xlviii) Implied because the power to grant permissions should naturally include power to revoke them.

12. ***It must be possible to verify system functionality, providing a transparent transparency system***

(xlix) *"for general application of open standards the "comply or explain, and commit" principle will be applied to orders from Central Government departments [...]"* [72, p.9] Open standards should be used unless it can be explained that an exception is necessary.

(l) *"Gemeenten maken gebruik van de open standaarden zoals vastgesteld door het College Standaardisatie en werken hierbij volgens het principe "pas toe of leg uit". Bij aanbestedingen van software krijgt, bij gelijke geschiktheid, open source de voorkeur"* [6, p.21]

Open standards should be used unless it can be explained that an exception is necessary. Open source is also encouraged and should be given preference when software is otherwise equal.

(li) *"[. . .] the government will work towards maximising the use of open standards for ICT systems for communication with citizens and businesses. In the associated "programme of headlines" the government applies the following starting points: Supplier-independence, Interoperability, Transparency, Checkability and Manageability and Digital sustainability."* [35, p.22] The advantages of open standards have multiple starting points that overlap with other requirements.

(lii) Implied in the context of transparency and the open design of the system. It is interesting to note that the interface specification and system requirements are all publicly documented. Some documents are even available under a Creative Commons license, for example publications from The Standardisation Forum [26][28].

13. ***Data stored in the system must only be accessible to users and agencies that are authorized***

(liii) See references (xxxiii), (xxxiv), and (xxiv)

(liv) Implied by the definition of 'Authorization'.

14. ***Agencies can read and write data to each user within the agency namespace by default***

(lv) See reference (xxviii)

(lvi) Implied because agencies need to provide data write access is needed, and since users need to be able to give permissions the sensible default is to allow an agency only access to the data they have provided by default.

(lvii) Existing functionality from MijnOverheid currently relies on this feature. Not allowing default write access to a separate namespace per agency would break basic functionality.

15. ***An agency can request a user to allow access to personal data or data written by another agency***

(lviii) *"Verder onderschrijft UWV met de inspectie SZW het belang van transparantie, maar ziet het meer en betere mogelijkheden door transparantie te integreren in de actieve dienstverlening aan de burger. De inspectie meent dat dit zeker bijdraagt aan transparantie, maar vraagt zich af of dit voldoende is. Het is namelijk voor de inspectie niet duidelijk geworden hoe volledig het beeld is dat de burger hiermee wordt gegeven van de informatie-uitwisselingen en -bewerkingen."* [74, p.28] Existing functionality for data exchange without explicit permission (trough Suwinet e.a.) is not yet entirely transparent. Citizens should be able to see which agencies can access their data.

(lix) Implied by the need for the user to give permission to allow access to data. To facilitate access requests an agency needs to let the user know they need access to data. This can be communicated in person, by mail, or electronically trough the system. The electronic option has obvious benefits since the origin of the request can be validated and the consequence of granting the request is immediately visible in the system.

16. ***Users can to issue temporary permissions to other users or agencies***

    (lx) See references (xl), and (xlvi)

    (lxi) Implied because granting and revoking is possible. It is common security practice to reissue certificates on a regular basis, with signed permissions this means that permissions should also be reissued regularly and thus have an implicit expiration date.

17. ***Additional keys can be created that are authenticated descendants or alternatives to the first government-issued ID***

    (lxii) *"Niveau 4 STORK betreft de toepassing van de Public Key Infrastructure (PKI). De persoon die zich identificeert doet dit met het persoonsgebonden certificaat van het middel. De authenticatie is erop gebaseerd dat met de private sleutel van het certificaat een technische ondertekening plaatsvindt van het authenticatieverzoek en dat de dienstaanbieder de mogelijkheid heeft via een publieke sleutel de geldigheid van de ondertekening (van het authenticatieverzoek) en het certificaat te controleren en de attributen hiervan in te zien (dat kan bijvoorbeeld enkel een nummer zijn of, afhankelijk van de rechten van de dienstaanbieder, de naam of leeftijd van certificaathouder). Op de niveaus tot en met 3 STORK vindt de authenticatie plaats met toepassing van Security Assertion Markup Language (SAML). Dit is een berichtenprotocol voor het uitwisselen authenticatie- en autorisatiegegevens tussen gebruikers van elektronische diensten, vertrouwensdienstverleners (authenticatie-, machtigings- en tekendiensten) en elektronische dienstaanbieders. De gebruiker die zich identificeert doet dit met een persoonsgebonden nummer van het middel. De authenticatie is erop gebaseerd dat de authenticatiedienst die het middel heeft uitgegeven, de dienstaanbieder een identiteits- of attribuutverklaring verstrekt. In de verklaring kan het nummer van het authenticatiemiddel zijn opgenomen (identiteitsverklaring), maar afhankelijk van de rechten van de dienstaanbieder kunnen in de verklaring ook gegevens van de gebruiker zijn opgenomen, zoals zijn naam, leeftijd of bevoegdheid (attribuutverklaring)."* [29, p.30] STORK 4 will use the PKI infrastructure. Until STORK 3 the SAML identity provider infrastructure will be used. Authentication is based on multiple provate identity providers, which consist of businesses that are trusted to issue new PIV cards.

    (lxiii) *"Zoals eerder in paragraaf 2.1 is uiteengezet, is technisch tekenen mogelijk met een certificaat. De persoon van de ondertekenaar kan dan via PKI worden achterhaald. Technisch tekenen is in beginsel mogelijk zonder certificaat van een eindgebruiker.*

Ook is een combinatie mogelijk authenticatie gebaseerd op SAML-berichtenverkeer en de toepassing van PKI. Hiervan is bijvoorbeeld sprake bij de PKI-signing van attribuutverklaringen." [27, p.11] The PKI infrastructure (possibly combined with the SAML infrastructure) can be used to identify the person that performed a signature.

(lxiv) *"Daarnaast worden er ook tests uitgevoerd bij toetreding, zal met pseudoniemen worden gewerkt in het berichtenverkeer en wordt gebruik gemaakt van vertrouwde certificaten."* [33, p.6] Message exchange can be performed under pseudonyms and using trusted certificates will be used.

(lxv) *"een besluit van BZK, dat de taakopdracht met betrekking tot het BSN-koppelregister behelst. Laatstgenoemde voorziening maakt het mogelijk dat private middelen in het publieke domein kunnen worden gebruikt, naast het publieke middel DigiD. In het BSN-koppelregister wordt (eenmalig) het BSN aan het pseudo-id van het private middel gekoppeld."* [35, p.46] Privately owned identity providers can be used next to the existing DigiD. In the BSN link register a persistent link is stored between the pseudo-id and the BSN.

18. ***Users can be identified with multiple persistent pseudonyms instead of only their BSN***

(lxvi) See references (lxiv), and (lxv).

(lxvii) *"Een eID-middel in het kader van het stelsel bevat een uniek identificerend pseudoniem. Bij gebruik van een publiek eID-middel (zoals de DigiD-kaart) in het private domein wordt geen BSN uitgewisseld, maar een pseudoniem dat per dienstaanbieder uniek is. Bij gebruik van de DigiD-kaart of een privaat eID-middel (bijvoorbeeld een bankpas) in het publieke domein wordt het pseudoniem vertaald in een BSN. Dit wordt in een door de overheid beheerd koppelregister bij gehouden, zoals nu ook in het huidige DigiD. In dit register worden ook private authenticatiemiddelen gekoppeld aan het BSN. Vanwege de verwerking van het BSN is het in stand houden van deze voorziening een exclusieve publieke taak."* [34, p.7] For communicating with businesses users can use a pseudonym that is unique to the business. It is the task of the government to maintain the mapping between pseudonyms and BSNs.

(lxviii) *"Het uitgeven van persoonsgebonden pseudoniemen."* [29, p.23] A requirement for the eID system is the ussuance of personal pseudonyms.

(lxix) *"Daarbij kan bijvoorbeeld concreet gedacht worden aan huidige uitdagingen voor gemeenten in het kader van de decentralisaties, gegevensuitwisseling binnen het stelsel van basisregistraties en privacy by design (structureel aandacht besteden aan privacyverhogende maatregelen) en pseudonimisering (versleuteling van identificerende gegevens, zoals bijvoorbeeld het burgerservicenummer) binnen het afsprakenstelsel eID."* [35, p.36] Data exchange within the system takes place according to *"privacy by design"* and supports pseudonymisation to hide identifying data such as BSN.

In order to evaluate how well the proposed solution fits the research question we evaluate how well the proposed system design satisfies the following 12 generic requirements:

1. ***Auditable*** *(log everything as part of the design)*
2. ***Authorization*** *(grant/revoke access only to those while they need it)*
3. ***Authentication*** *(credentials are inherently checked)*
4. ***Decentralized*** *(less central control, and allow the network to grow)*
5. ***Empowering individuals*** *(user has the final say who can use their data)*
6. ***Encryption*** *(future proof with strong encryption, allowing flexibility)*
7. ***Indexed*** *(searchable without leaking data about the population)*
8. ***Privacy protecting*** *(the system should foster privacy by design)*
9. ***Public/Private keys*** *(with the ability to use hardware tokens)*
10. ***Scalable*** *(to at least the size of a country, in the PiB range)*
11. ***Transparent*** *(a user has complete insight in his/her data stored)*
12. ***User-centric*** *(ease of use to allow user control over data)*

The following list contains the initial design thoughts that influenced the project. Note that while these influenced the proposed design as an inspiration, they in no way represent the final outcome in this report. These design thoughts are included because for the sake of completeness.

- OS3 (Open Standards, Open Software, Open Security) design that should be tailored to local needs, but flexible to be used for other purposes.
- Distributing both the access keys and the data seems the best way to create a fully transparent system without sacrificing privacy or security.
- Authorization should be given by the user. This can be to a (sub)organization. This signed authorization should have an expiration date (with system wide maximum time enforced by the servers).
- Encryption keys are made available to users by encrypting them with their public key, more than one person can have access to the same encryption keys.
- Data can safely be stored on any cloud storage platform since it is strongly encrypted. The system should however be agnostic to the type of storage to allow political decision to be made to move the data. The system should be easily extendable to allow storage of data on alternate platforms.
- Access logs should processed in a timely fashion and stored in historical records in the tree with the relevant data. There are concerns that access logs may allow (partial) reconstruction of deleted data, to prevent this a mechanism to remove access logs are removed as well preventing
- All queries to central servers are signed (some twice for queries 'on behalf of') and must contain a token to prevent replay attacks.
- Any PIV card (smartcard) capable of X.509 should be able to be used, as long as the CA is on a trusted list. This can be *'PKI overheid'*, or the future *'Identiteitsbewijs'* with this capability.
- Data is segmented in the data structure which is a NoSQL database containing metadata for the entire tree, and the encrypted blob storage which is used to store vast quantities of data.
- The content of the distributed database should be semi-public, and the encrypted blob storage should be fully public without compromising the security of the system. As long as keys are kept private the system functions as designed.
- Tree has list of 'servers', 'organizations', 'persons', 'keys', 'templates'. All data structures are stored in this tree, which has an ACL on each folder. Small metadata can be stored directly in this tree, but all large files are pointers to the encrypted blobs. The min/max size is determined system wide.

- While it is impossible to prevent government agencies from aggregating all citizen data into their own centralized database (for the purpose of monitoring citizens) this system should be designed to make it very hard to use for that purpose.

- The system should be practical to use both for the users as well as the government agencies that need to aggregate data into it. By offering a design for a practical solution that provides transparency without a large cost in privacy and/or security

Benchmarks were performed on an Intel i7-3537U CPU clocked at 2Ghz.
The Firefox version 44 browser was used for the CryptoJS benchmarks.
A Yubikey NEO[1] was used for the PIV RSA benchmarks.

TABLE F.1: RSA performance benchmark

Operation	**Native (openssl on i7 CPU)**	**CryptoJS**	**Smart Card**
Signing	5.5 msec	41.8 msec (7 × *slower*)	1.68 sec (300 × *slower*)
Verifying	3.2 msec	4.8 msec (1.5 × *slower*)	native (1 × *speed*)

PIV signing benchmark example

```
openssl sha256 -binary test.txt > test.sha256
pkcs15-crypt --sign --key 2 --pkcs1 --sha-256 --input test.sha256 --raw
    --output test.signature --pin $PIN

REPEATED 100x! 0.19user 0.42system 2:47.95elapsed 0%CPU
REPEATED 100x! 0.22user 0.39system 2:49.33elapsed 0%CPU
REPEATED 100x! 0.41user 0.54system 2:48.11elapsed 0%CPU

Average = (167.95+169.33+168.11)/300 = 1,684633333 sec.
```

TABLE F.2: AES performance benchmark

Operation	**Native (openssl on i7 CPU)**	**CryptoJS**
Encrypt/Decrypt	109 MB/s	23 MB/s (4.7 × *slower*)

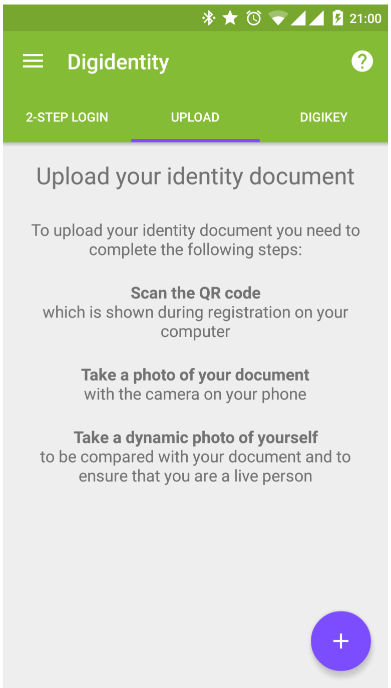
AES OpenSSL benchmark example

```
openssl enc -aes-256-ctr -e -K $KEY -iv $IV -in test.txt -out test.dat

ENCRYPTED 1024 MB! 2.90user 6.95system 0:09.95elapsed 98%CPU
ENCRYPTED 1024 MB! 2.61user 6.38system 0:09.02elapsed 99%CPU
ENCRYPTED 1024 MB! 2.82user 6.28system 0:09.17elapsed 99%CPU

Average = (9.95+9,02+9.17)/3072 = 0,009160156 = 109 MB/s
```

[1] https://www.yubico.com/products/yubikey-hardware/yubikey-neo/



Upload your identity document

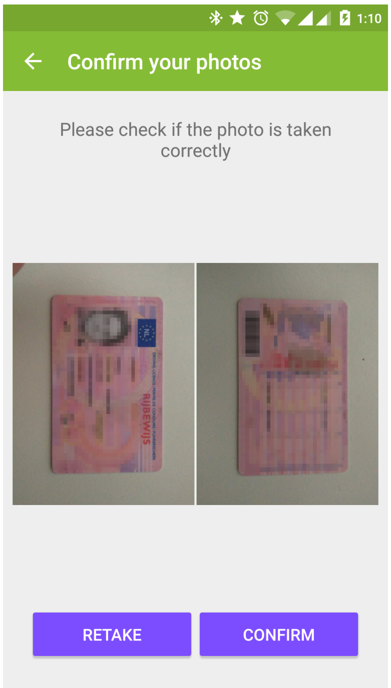
To upload your identity document you need to complete the following steps:

Scan the QR code
which is shown during registration on your computer

Take a photo of your document
with the camera on your phone

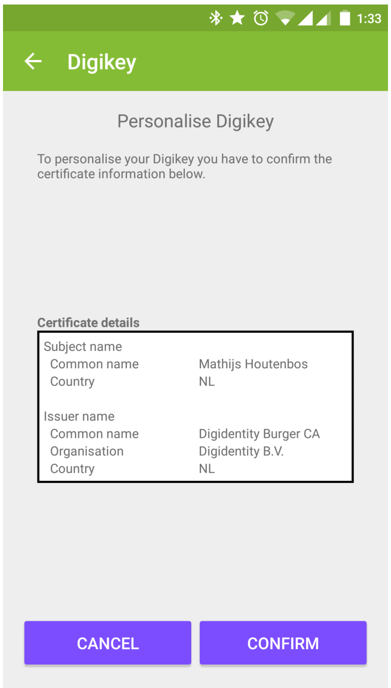
Take a dynamic photo of yourself
to be compared with your document and to ensure that you are a live person

FIGURE G.1: Digidentity instructions for registration



Please check if the photo is taken correctly

FIGURE G.2: Scanning a photo ID both front and back



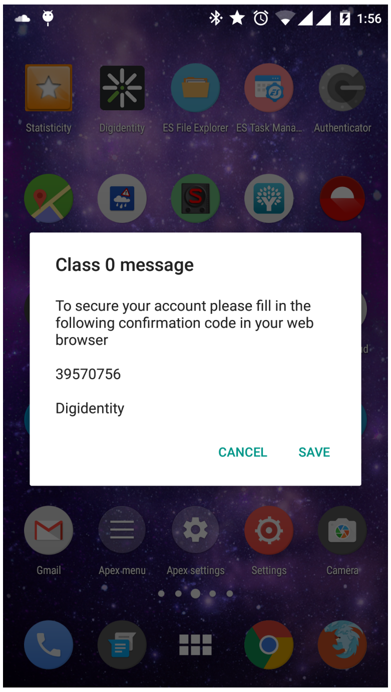
Personalise Digikey

To personalise your Digikey you have to confirm the certificate information below.

Certificate details

Subject name	
Common name	Mathijs Houtenbos
Country	NL
Issuer name	
Common name	Digidentity Burger CA
Organisation	Digidentity B.V.
Country	NL

FIGURE G.3: Digidentity Digikey certificate request confirmation



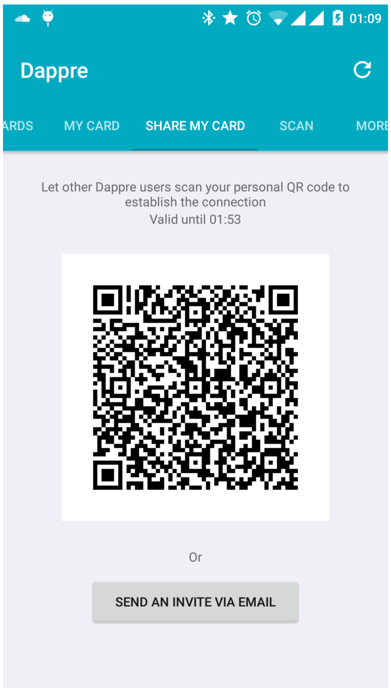
Class 0 message

To secure your account please fill in the following confirmation code in your web browser

39570756

Digidentity

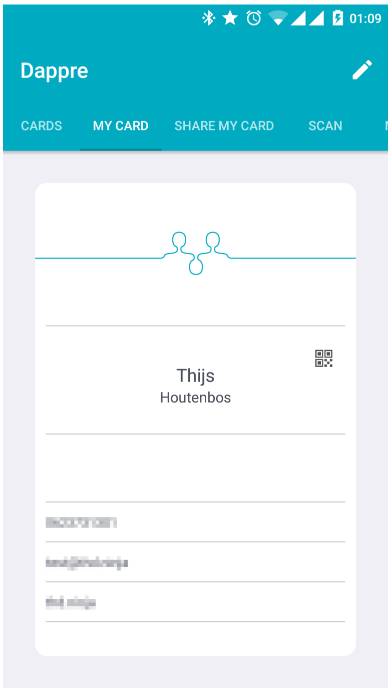
FIGURE G.4: Receiving the Class 0 SMS code for phone confirmation



Let other Dappre users scan your personal QR code to establish the connection
Valid until 01:53

Or

FIGURE H.1: Dappre QR code used to link to another user



Thijs
Houtenbos

[redacted]

[redacted]

[redacted]

FIGURE H.2: Personal information card that is being shared

Bibliography

[1] R Plasterk. “Visiebrief digitale overheid 2017”. In: (2013), pp. 1–8. URL: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2013/05/23/visiebrief-digitale-overheid-2017/visiebrief-digitale-overheid-2017.pdf.

[2] VDP. “Overheidsbrede Dienstverlening 2020”. In: *Deze publicatie is tot stand gekomen in samenwerking met: Belastingdienst, Divosa, DUO, Informatie Management Groep, King, Manifestgroep, Ministeries van BZK, Financiën, EZ, NVVB, Hiemstra en de Vries, Social Impact, SVB, Top- kring Dienstverlening Gemeen* 1 (2014), pp. 1–20. URL: http://www.publieksdiensten.nl/wp-content/uploads/2014/03/OverheidsbredeDienstverlening2020.pdf.

[3] M.J.M. Verhagen. “Digitale Agenda.nl”. In: (2011). URL: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2011/05/17/digitale-agendanl/digitale-agendanl.pdf.

[4] Ministerie van Economische Zaken Landbouw en Innovatie. “Digitale Implementatie Agenda.nl”. In: (2011). URL: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2011/12/13/digitale-implementatie-agenda-nl/120123-mez011-digitale-impl-agenda-finale-versie.pdf.

[5] Bestuurlijk Overleg van rijk provincies gemeenten en waterschappen. “Uitvoeringsprogramma Dienstverlening En E-Overheid - “BURGER EN BEDRIJF CENTRAAL””. in: december (2008), pp. 1–76. URL: http://www.digitaleoverheid.nl/images/stories/over_het_NUP/nup-versie-2-0-1-12-versie.pdf.

[6] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. “Overheidsbrede implementatieagenda voor dienstverlening en e-overheid (i-NUP)”. in: (2011), p. 24. URL: http://www.digitaleoverheid.nl/images/stories/Publicaties/agenda_e-overheid_.pdf.

[7] Min. van BZK. “Eindrapport i-NUP”. in: December (2014). URL: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2014/12/01/eindrapport-i-nup/eindrapport-i-nup.pdf.

[8] M.J.M. Verhagen and Landbouw en Innovatie Minister van Economische Zaken. “Besluit van de Minister van Economische Zaken, Landbouw en Innovatie van 12 december 2011, nr. ETM/IT/11168229 tot instelling van het College Standaardisatie en het Forum Standaardisatie 2012 (Instellingsbesluit College en Forum Standaardisatie 2012)”. In: 23581 (2011), pp. 1–5. URL: https://zoek.officielebekendmakingen.nl/stcrt-2011-23581.pdf.

[9] R.H.A. Plasterk. “Regeling voorzieningen GDI”. in: *Staatscourant* 37158 (2015), pp. 1–12. URL: https://zoek.officielebekendmakingen.nl/stcrt-2015-37158.pdf.

[10] Nationaal Beraad Overheden. “Overheidsbrede implementatieagenda digitale dienstverlening 2017”. In: Versie 1.1.november 2015 (2015), pp. 1–54. URL: http://www.digitaleoverheid.nl/images/stories/digitaal2017/documenten/implementatieagenda-digitale-dienstverlening-2017-versie-1-1.pdf.

[11] Manifestgroep. “Werkboek Publieke Dienstverlening Werken aan de workshops”. In: December (2011), p. 76. URL: https://manifestgroep.pleio.nl/file/download/22672602.

[12] Ross Anderson et al. “Database State”. In: (2009). URL: https://www.cl.cam.ac.uk/$\sim$rja14/Papers/database-state.pdf.

[13] Chris Clifton and Don Marks. “Security and Privacy Implications of Data Mining”. In: *Data Mining and Knowledge Discovery* (1996), pp. 15–19. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.28.891&rep=rep1&type=pdf.

[14] John McCarthy and Peter Wright. *Technology as Experience*. 2004. ISBN: 0262134470. URL: https://www.researchgate.net/profile/Peter_Wright7/publication/224927635_Technology_as_Experience/links/00b7d51e2c675e1620000000.pdf.

[15] Kieron O’Hara. “Transparent Government , Not Transparent Citizens : A Report on Privacy and Transparency for the Cabinet Office”. In: (2011), pp. 1–84. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61279/transparency-and-privacy-review-annex-a.pdf.

[16] H. Gillebaard and Arthur Vankan. “De digitale (zelf)redzaamheid van de burger: ondersteuning bij de Digitale Overheid 2017”. In: (2013). URL: https://www.kb.nl/sites/default/files/digitale_zelfredzaamheid_burger.pdf.

[17] Nationale Ombudsman. “De burger gaat digitaal”. In: december (2013). URL: http://www.ey.com/Publication/vwLUAssets/Benchmark_digitale_dienstverlening_2013/$FILE/EY-Benchmark-digitale-dienstverlening-2013.pdf.

[18] Ernst and Young, Guill van den Boom, and Ad Buckens. “2017: een brug te ver? Benchmark digitale dienstverlening 2013”. In: (2013). URL: http://www.ey.com/Publication/vwLUAssets/Benchmark_digitale_dienstverlening_2013/$FILE/EY-Benchmark-digitale-dienstverlening-2013.pdf.

[19] Univerisy of Utah Honors Think Tank 2012. “Transparency and Privacy - Clashing Paradigms in a Web 2.0 World”. In: (2012). URL: http://honors.utah.edu/wp-content/uploads/Transparency-Privacy-Final-Report.pdf.

[20] Ann Cavoukian. “Privacy by Design - The 7 foundational principles - Implementation and mapping of fair information practices”. In: *Information and Privacy Commissioner of Ontario, Canada* (2009), p. 5. ISSN: 1876-0678. DOI: 10.1007/s12394-010-0062-y.

[21] Ann Cavoukian. “Privacy by Design”. In: *Identity in the Information Society* 3.2 (2010), pp. 1–12. ISSN: 1876-0678. DOI: 10.1007/s12394-010-0062-y. URL: https://iapp.org/media/presentations/11Summit/RealitiesHO1.pdf.

[22] Ann Cavoukian, Mark Dixon, and Oracle. “Privacy and Security by Design : An Enterprise Architecture Approach”. In: September

(2013). URL: https://www.ipc.on.ca/images/Resources/pbd-privacy-and-security-by-design-oracle.pdf.

[23] H.G.J. Kamp. “Voortgang wetgeving voor de e-overheid”. In: (2015). URL: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2015/06/29/kamerbrief-over-de-voortgang-wetgeving-voor-de-e-overheid/kamerbrief-over-de-voortgang-wetgeving-voor-de-e-overheid.pdf.

[24] R.H.A. Plasterk. “Uitgangspunten wetgeving Generieke Digitale Infrastructuur”. In: *Rijksoverheid* (2015). URL: https://vng.nl/files/vng/20151215-uitgangspunten-generieke-digitale-infrastructuur.pdf.

[25] The Standardisation Forum. “Assurance levels for authentication for electronic government services”. In: (2012). URL: https://www.forumstandaardisatie.nl/fileadmin/os/publicaties/HR_Betrouwbaarheidsniveaus_EN_WEB.pdf.

[26] The Standardisation Forum. “Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten”. In: versie 3 (2014). URL: https://www.forumstandaardisatie.nl/fileadmin/os/publicaties/HR_Betrouwbaarheidsniveaus_v3__2014_.pdf.

[27] Tweede kamer der Staten-generaal. “Wijziging van het Wetboek van Strafvordering en de Wet op de economische delicten in verband met het gebruik van elektronische processtukken (digitale processtukken Strafvordering); Memorie van toelichting; Memorie van toelichting”. In: 3 (2014), pp. 1–56. URL: https://www.eerstekamer.nl/behandeling/20141124/memorie_van_toelichting/document3/f=/vjp7ipudmfw2.pdf.

[28] D Krukkert. “Expert Recommendation - SAML v 2.0”. In: (2009). URL: https://www.forumstandaardisatie.nl/fileadmin/os/documenten/SAMLv2.0.pdf.

[29] Carlo Koch, Gerrit Jan van ‘t Eind, and Bart Schmidt. “Masterplan eID”. 2014. URL: http://www.eid-stelsel.nl/fileadmin/eid/documenten/Masterplan_eID_vs1_00_def.pdf.

[30] Bruce Schneier. “Two-Factor Authentication: Too Little, Too Late”. In: *Communications of the ACM* 48.4 (2005), p. 136. ISSN: 00010782. DOI: 10.1145/1053291.1053327. URL: http://www.itsec.gov.cn/webportal/download/2004_two-factor.pdf.

[31] Manal Adham et al. “How to attack two-factor authentication internet banking”. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 7859 LNCS (2013), pp. 322–328. ISSN: 03029743. DOI: 10.1007/978-3-642-39884-1_27. URL: http://fc13.ifca.ai/proc/9-3.pdf.

[32] Alexandra Dmitrienko et al. “Security analysis of mobile two-factor authentication schemes”. In: *Intel Technology Journal* 18.4 (2014), pp. 138–161. ISSN: 1535864X. URL: http://ezproxy.library.capella.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=97377858&site=ehost-live&scope=site.

[33] R.H.A. Plasterk. “Pilotvoorwaarden en pilotcriteria eID Stelsel Bij”. In: (2015). URL: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/

2015/06/30/kamerbrief-over-pilotvoorwaarden-en-pilotcriteria-eid/kamerbrief-over-pilotvoorwaarden-en-pilotcriteria-eid.pdf.

[34] Minister van Economische Zaken. "eID Stelsel en DigiD-kaart". In: (2013). URL: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2013/12/19/kamerbrief-over-eid-stelsel-en-digid-kaart/tweede-kamerbrief-eid.pdf.

[35] Bianca Rouwenhorst and Caroline Schoots. "Digiprogramma 2015". In: (2015). URL: https://www.digicommissaris.nl/media/attachment/2015/11/12/20150210_03b_01_oplegger_en_digiprogramma.pdf.

[36] Servicecentrum Logius. "Best Practices ebMS Digikoppeling 2.0". In: november (2011), pp. 1–22. URL: https://www.logius.nl/fileadmin/logius/product/digikoppeling/algemeen/Digikoppeling_Best_Practices_ebMS_v1.5.2_.pdf.

[37] Eric van den Hoek and Ton Laarhoven. "Early Adopters Berichtenbox MijnOverheid Sessie Techniek". In: april (2015). URL: https://www.logius.nl/fileadmin/logius/ns/diensten/mijnoverheid/evenementen/Early_Adopters__Techniek_15-04-15.pdf.

[38] Willeke Schouls and Ton Laarhoven. "Berichtenbox MijnOverheid (Techniek)". In: september (2015). URL: http://docplayer.nl/storage/26/7064743/1454622223/Kzcob3qUZtC7KG2jtHTp1A/7064743.pdf.

[39] IETF. "RFC 6238 - TOTP: Time-Based One-Time Password Algorithm". In: (2011). ISSN: 0717-6163. URL: https://tools.ietf.org/pdf/rfc6238.pdf.

[40] Hang Zhang, Dongdong She, and Zhiyun Qian. "Android Root and Its Providers: A Double-Edged Sword". In: *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS)* (2015), pp. 1093–1104. ISSN: 15437221. DOI: 10.1145/2810103.2813714. URL: http://www.cs.ucr.edu/$\sim$zhiyunq/pub/ccs15_root_providers.pdf.

[41] Wen Xu. "Ah! universal android rooting is back". In: (2015). URL: https://www.blackhat.com/docs/us-15/materials/us-15-Xu-Ah-Universal-Android-Rooting-Is-Back.pdf.

[42] Jan Fraanje and Qiy. "Qiy – pilot persoonlijk digitaal domein: 'de burger centraal'." In: (2015). URL: https://www.boxtel.nl/fileadmin/Bestuur/College/Besluitenlijsten2015/01_januari/27-01-2015/02.08_150122_OpzetProjectplanQiy-GemeentelijkDomein_S_15.0001175_1.pdf.

[43] NIST. "FIPS PUB 201-2 FEDERAL". in: August (2013). URL: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf.

[44] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. "Interface Specifications EID SCHEME". 2014. URL: http://www.eid-stelsel.nl/fileadmin/eid/documenten/4._Interface_specifications_v1.0.pdf.

[45] R. L. Rivest, A. Shamir, and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems". In: *Communications of the ACM* 21.2 (1978), pp. 120–126. ISSN: 00010782. DOI: 10.1145/359340.359342. URL: https://people.csail.mit.edu/rivest/Rsapaper.pdf.

[46] Cooper et. al. and IETF. "RFC 5280". In: (2008). URL: https://tools.ietf.org/pdf/rfc5280.pdf.

[47] FIDO Alliance. “FIDO U2F Javascript API”. in: (2014).

[48] Hannes Tschofenig. “Web Cryptography: Supporting the FIDO Protocol Family”. In: September 2014 (2014), pp. 10–11. URL: https://www.w3.org/2012/webcrypto/webcrypto-next-workshop/papers/webcrypto2014_submission_1.pdf.

[49] Carl Ellison and Bruce Schneier. “Ten Risks of PKI: What You’re not Being Told about Public Key Infrastructure”. In: *CRYPTOGRAPHY* 16.1 (2000), pp. 1–8. URL: https://www.schneier.com/cryptography/paperfiles/paper-pki.pdf.

[50] Rick Cattell. “Scalable SQL and NoSQL data stores”. In: *ACM SIGMOD Record* 39.4 (2011), p. 12. ISSN: 01635808. DOI: 10.1145/1978915.1978919. URL: http://www.cattell.net/datastores/Datastores.pdf.

[51] Werner Vogels. “Eventually Consistent”. In: *Queue* 6.6 (2008), p. 14. ISSN: 15427730. DOI: 10.1145/1466443.1466448. URL: http://web.stanford.edu/class/cs345d-01/rl/eventually-consistent.pdf.

[52] Guido J. van ‘t Noordende et al. “A Trusted Data Storage Infrastructure for Grid-Based Medical Applications”. In: *International Journal of Grid and High Performance Computing* 1.2 (2009), pp. 1–14. URL: ATrustedDataStorageInfrastructureforGrid-BasedMedicalApplications.

[53] Anthony Harrington and Christian Jensen. “Cryptographic access control in a distributed file system”. In: *ACM SIGOPS Symposium on Access Control Models and Technologies* (2003), pp. 158–165. URL: http://portal.acm.org/citation.cfm?id=775432.

[54] Shucheng Yu et al. “Achieving secure,scalable ,and fine-grained data access control in cloud computing”. In: *Ieee Infocom* (2010), pp. 1–9. ISSN: 0743-166X. DOI: 10.1109/INFCOM.2010.5462174. URL: http://www.acsu.buffalo.edu/$\sim$kuiren/ubisec/INFOCOM10-sharing.pdf.

[55] Giuseppe Ateniese et al. “Improved proxy re-encryption schemes with applications to secure distributed storage”. In: *ACM Transactions on Information and System Security* 9.1 (2006), pp. 1–30. ISSN: 1094-9224. DOI: 10.1145/1127345.1127346. URL: https://eprint.iacr.org/2005/028.pdf.

[56] Forum Standaardisatie. “Open Document Standards for the Government Guide”. In: april (2011). URL: https://www.forumstandaardisatie.nl/fileadmin/os/documenten/Handreiking_ODF_Engelse_versie.pdf.

[57] E J A Folmer and L M Punter. “Expert Recommendation new versions Open Document Format”. In: August (2011). URL: https://www.forumstandaardisatie.nl/fileadmin/os/documenten/Expert_recommendation_odf_2013.pdf.

[58] Erika Hokke and Standardisation Forum. “Expert recommendation on NEN-ISO 19005-1:2005 (PDF/A-1)”. In: (2008). URL: https://www.forumstandaardisatie.nl/fileadmin/os/documenten/NEN-ISO19005-12005PDFA-1.pdf.

[59] J.P.C. Verhoosel and M. van Bekkum. “Expert Recommendation - ISO 32000-1:2008, Part 1: PDF 1.7”. In: August (2009). URL: https://www.forumstandaardisatie.nl/fileadmin/os/documenten/PDFExpertadviesUK.pdf.

[60] M. Belshe et al. "RFC 7540 - Hypertext Transfer Protocol Version 2 (HTTP/2) Abstract". 2015. URL: https://tools.ietf.org/pdf/rfc7540.pdf.

[61] R. (Telematica Instituut) Arends et al. "RFC 4033 - DNS Security Introduction and Requirements". In: *IETF* (2005). URL: https://tools.ietf.org/pdf/rfc4033.pdf.

[62] B. Laurie et al. "RFC 5155 - DNS Security (DNSSEC) Hashed Authenticated Denial of Existence". 2008. URL: https://tools.ietf.org/pdf/rfc5155.pdf.

[63] Meltem Sönmez Turan et al. "Recommendation for Password-Based Key Derivation - Part 1: Storage Applications". In: *NIST Special Publication* December (2010), p. 14. URL: http://csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf\nhttp://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Recommendation+for+Password-Based+Key+Derivation+Part+1+:+Storage+Applications#2.

[64] C Percival. "Stronger key derivation via sequential memory-hard functions". In: *Self-published* (2009), pp. 1–16. URL: https://www.tarsnap.com/scrypt/scrypt.pdf.

[65] H. Krawczyk (IBM), M. Bellare (UCSD), and R. Canetti (IBM). "RFC 2104 - HMAC: Keyed-Hashing for Message Authentication Status". 1997. URL: https://tools.ietf.org/pdf/rfc2104.pdf.

[66] Radia Perlman. "An Overview of P K I Trust Models". In: *IEEE Network* 13.6 (1999), pp. 38–43. DOI: 10.1109/65.806987.

[67] Guido van 't Noordende. "Beyond informed consent: practical approaches for managing consent and fine-grained authorization in large-scale electronic medical record systems." In: (2011). URL: https://staff.fnwi.uva.nl/g.j.vantnoordende/publications/ps/cpdp2011_submission_28.pdf.

[68] Emily Stark, Michael Hamburg, and Dan Boneh. "Symmetric cryptography in javascript". In: *Proceedings - Annual Computer Security Applications Conference, ACSAC* (2009), pp. 373–381. ISSN: 10639527. DOI: 10.1109/ACSAC.2009.42. URL: https://bitwiseshiftleft.github.io/sjcl/acsac.pdf.

[69] Harry Halpin. "The W3C Web Cryptography API : Motivation and Overview". In: *Www* (2014), pp. 959–964. DOI: 10.1145/2567948.2579224. URL: http://ws-rest.org/2014/sites/default/files/wsrest2014_submission_11.pdf.

[70] Leonel João Fernandes Braga. "Web Browser Access to Cryptographic Hardware". In: (2012). URL: http://mei.di.uminho.pt/sites/default/files/dissertacoes/eeum_di_dissertacao_pg17311.pdf.

[71] Ivan Risti. "SSL / TLS Deployment Best Practices". In: 3.September (2013), pp. 1–11. URL: https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices.pdf.

[72] Ministry of Economic Affairs. "The Netherlands in Open Connection". In: (2007). URL: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/brochures/2007/12/20/the-netherlands-in-open-connection/nl-in-open-connection.pdf.

[73] SVB and De Argumentenfabriek. “De Burgerpolis: zicht op zekerheid”. In: (2009). URL: http://www.onderzoekwerkeninkomen.nl/rapporten/nk0yl92p/de-burgerpolis-zicht-op-zekerheid.pdf.

[74] J.A. van den Bos (SZW). *Brief programmarapportage "De burger bediend in 2013"*. 2013. URL: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2013/11/08/programmarapportage-de-burger-bediend-in-2013/programmarapportage-de-burger-bediend-in-2013.pdf.

[75] R.H.A. Plasterk. “Aanbieding eindverslag i-NUP”. in: *Rijksoverheid* (2015), pp. 1–8. URL: http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2015/02/06/kamerbrief-over-verbeteren-kwaliteit-en-betaalbaarheid-zorg.html.

[76] Vereniging van Nederlanse Gemeenten. “Dienstverlening draait om mensen”. In: (2010). URL: https://vng.nl/files/vng/publicaties/2012/20100310_dienstverlening_draait_om_mensen_.pdf.

[77] Manifestgroep. “Werkboek Publieke Dienstverlening Werken aan inzicht in dienstverlening”. In: December (2011), p. 76. URL: https://manifestgroep.pleio.nl/file/download/22672622.

[78] Logius. “Koppelvlakspecificaties Berichtenbox – MijnOverheid”. In: (2015). URL: https://www.logius.nl/fileadmin/logius/ns/diensten/mijnoverheid/koppelvlakspecificaties/Koppelvlakspecificaties_Berichtenbox_v1.9.pdf.

[79] R.H.A. Plasterk. “Voortgang eID”. in: *Rijksoverheid* (2014). URL: http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2015/02/06/kamerbrief-over-verbeteren-kwaliteit-en-betaalbaarheid-zorg.html.