When Willeke can get rid of paperwork: a lean infrastructure for qualified information exchange based on trusted identities

Sander Dijkhuis
Cleverbase
The Hague, The Netherlands
sander.dijkhuis@cleverbase.com

Remco van Wijk
Cleverbase
The Hague, The Netherlands
remco.van.wijk@cleverbase.com

Hidde Dorhout
Smart Data Company
The Hague, The Netherlands
hdorhout@gmail.com

Nitesh Bharosa
Delft University of Technology
Delft, The Netherlands
n.bharosa@tudelft.nl

ABSTRACT

As a frequent participant in eSociety, Willeke is often preoccupied with paperwork because there is no easy to use, affordable way to act as a qualified person in the digital world. Confidential interactions take place over insecure channels like e-mail and post. This situation poses risks and costs for service providers, civilians and governments, while goals regarding confidentiality and privacy are not always met. The objective of this paper is to demonstrate an alternative architecture in which identifying persons, exchanging information, authorizing external parties and signing documents will become more user-friendly and secure. As a starting point, each person has their personal data space, provided by a qualified trust service provider that also issues a high level of assurance electronic ID. Three main building blocks are required: (1) secure exchange between the personal data space of each person, (2) coordination functionalities provided by a token based infrastructure, and (3) governance over this infrastructure. Following the design science research approach, we developed prototypes of the building blocks that we will pilot in practice. Policy makers and practitioners that want to enable Willeke to get rid of her paperwork can find guidance throughout this paper and are welcome to join the pilots in the Netherlands.

CCS CONCEPTS

• **Computer systems organization** → *Cloud computing*;

KEYWORDS

Qualified information exchange, digital infrastructures, personal data management, distributed systems, privacy, data minimisation, authentication, authorisation, data portability, EIDAS, GDPR

ACM Reference Format:
Sander Dijkhuis, Remco van Wijk, Hidde Dorhout, and Nitesh Bharosa. 2018. When Willeke can get rid of paperwork: a lean infrastructure for qualified information exchange based on trusted identities. In *Proceedings of 19th Annual International Conference on Digital Government Research (dg.o'18),* Anneke Zuiderwijk and Charles C. Hinnant (Eds.). ACM, New York, NY, USA, Article 4, 10 pages.

dg.o'18, June 2018, Delft, Nl

1 INTRODUCTION

Meet Willeke, a fictional character that personifies the interactions of a citizen in our eSociety. Willeke leads a busy life and does her Christmas shopping online, as well as most of her freelance work. For her business, she can do more and more formal interactions with the Dutch government online, such as filing sales tax returns on the Tax Office portal and requesting permits using a standardised login scheme. However, she frequently has to print contracts on paper, sign these with 'wet signatures' (pen and ink), and deliver these using postal services. She's somewhat happy that retrieving her medical records still requires physical identification at the doctor's office, instead of logging in to an insecure online portal.

Sometimes Willeke is shocked to see the private information others are sharing with her over an unsafe channel such as email [12]. Over the years, our eSociety — referring to the coexistence of several e-communities such as e-business, e-government and e-health that use information and communication technologies (ICT) in order to facilitate interactions — has gained traction. Due to major investments and standardization efforts, many types of interactions (e.g. online sales and access to public services) have undergone transformations that harness the potential of information technologies. The latest analysis of ICT developments from the International Telecommunication Union [10] shows that the availability, access and use of internet communication has grown substantially over the past decade, resulting in more persons online than ever before (almost 4 billion). Social media usage and online sales are breaking record numbers and many people like Willeke reap the benefits. Surely, this is progress. However, as we have already stated in the case of Willeke, there are still some concerns.

First, there is the concern of provider centricity. Giovanni Buttarelli, the European Data Protection Supervisor (EDPS), warns[1]: *"Our online lives currently operate in a provider-centric system, where privacy policies tend to serve the interests of the provider or of a third party, rather than the individual. This makes it difficult for individuals to exercise their rights or manage their personal data online. A more*

[1] https://edps.europa.eu/press-publications/press-news/press-releases/2016/towards-new-reality-taking-back-control-our-online_en

human-centric approach is needed which empowers individuals to control how their personal data is collected and shared."

Second, when high levels of assurance are needed, information processes in society are often not very "e". In many business and government processes, paper statements still play an essential part of the processes. Automation is limited to the transport of scanned documents. For example, to apply for a mortgage in the Netherlands, an employer's declaration is required on paper with either a business stamp or a letter with a 'wet signature' stating that the company does not possess a business stamp. Citizens often receive letters at their home address to facilitate digital processes. For many parties post is a more trustworthy addressing system than e-mail. An example is the pre-completed tax return process in the Netherlands (we come back to this example in Section 4 of this paper). Although such paper-based loops help satisfy requirements for authentication and authorisation, they are costly and pose risks such as a undetectable data breach (e.g., letter opened by someone else who then disposes it). Alternatively, the use of e-mail in formal interactions provide opportunities for social engineering and identity fraud. Sometimes, when funds are available, organisations invest in secured digital portals and expect that persons use them in formal interactions. Yet, in practice, many do not even know the portal exists until sanctions follow. Examples include the use of portals of the Office of Education in the Netherlands[2] and the use of the digital post-box of the Dutch Government[3].

To sum up, our problem statement is that current eSociety is provider-centric and flawed when it comes to information exchange, in particular in formal transactions that require a high degree of certainty about the identity or expressions of people when accessing private or confidential information online. The flawed design exposes persons to risks, not only regarding data leaks, social engineering and identity fraud, but also when it comes to legal certainty (proof of compliance to the information requests). Zooming in on this problem statement, we claim that the common barrier for human centricity and a sound design for qualified information exchange (QIE) is the lack of affordable and easy to use digital identities (eIDs). The main proposition of this paper is that as soon as affordable and easy to use eID solutions are provided for authentication and creating qualified signatures, the barrier will be removed.

2 RESEARCH APPROACH

Striving to achieve the objective stated in the introduction (i.e. present a substantiated and tested solution for a human centric and cross-domain QIE), we employ the design science research approach [9]. This approach provides the procedure that guides us through the processes of real world problem analysis, theoretical exploration, design and the development and evaluation of (designed) artifacts with the explicit intention of improving the performance and value of the artifact. Such artifacts include constructs, models, methods, and instantiations (i.e. deploy, run and use the artifact). The central artifact of this research is the architecture of a digital infrastructure for QIE. Following the design science procedure proposed by Peffers et al. [15], this research includes the following six steps:

(1) Problem identification and motivation. Triggered by prior research [3, 17], a small team of three practitioners and one researcher collaborated on how to move to the next level in eSociety.
(2) Definition of the objectives for a solution. Based on the problem statement, we inferred the objectives of a solution from the problem definition and knowledge of what is possible and feasible (based on literature review and several analysis workshops). The objectives for our solution are qualitative: enable human centric and qualified information exchange in the most generic, easy to implement and flexible manner possible. From June to August 2017, a total of six analysis workshops focused on pinpointing the problem areas. The workshops were performed with a small multidisciplinary team of four to six persons. Section 5 (diagnosis) summarizes the main results of the analysis workshops.
(3) Design and development of the artifacts. This step focused on determining the artifact's desired functionality and its architecture and then creating the actual artifact. This required a combination of design workshops and software programming sessions. For six months, 0.3 FTE has worked on the basic exchange infrastructure — we call this the qualified ring — and the qualified trust service provider's tool set. Subsequently, seven people in a two-day sprint developed a working prototype that supports multiple games. The conceptual framework used for design is based on the work of van Wijk et al. [6, 17] (discussed in Section 4) as well as the eIDAS regulation set by European Parliament and the Council on electronic identification and trust services for electronic transactions [6].
(4) Demonstration. We demonstrate how information games can be facilitated using prototypes of a personal data space and a qualified ring. This involves its use in experimentation (simulation) based on a simple and a complex real-world case (Section 5).
(5) Evaluation. Using a two-day pressure cooker (workshop) session in December 2017 (with the entire design team), we simulated and observed how well the prototype works a solution for human centricity and a sound design for qualified information exchange. This activity involves comparing the objectives of a solution to actual observed results from use of the prototype. Conceptually, the simulation resulted in experimental evidence or proof that the solutions works as intended. Section 7 discusses the results of the evaluation. Once the prototypes are ready for end-user testing, we will evaluate them with end-users.
(6) Communication. Finally, this paper is a first means of communicating this research externally. Even while there are still open questions for future research, the current results present opportunities for realising a more human centric eSociety.

Throughout these research steps, multiple instances of the three cycles — relevance, rigor and design — [9] were completed, underlining the iterative nature of the presented research.

[2] https://nos.nl/op3/artikel/2165437-wie-kijkt-er-nou-op-mijnduo.html
[3] https://nos.nl/artikel/2191693-aanmaningen-boetes-mensen-missen-massaal-digitale-post-van-overheid.htm

3 CONCEPTUAL FRAMEWORK: QUALIFIED INFORMATION EXCHANGE

Our conceptual framework draws on the work by van Wijk et al [6] on qualified information exchange (QIE) as well as the eIDAS regulation set by European Parliament and of the Council on electronic identification and trust services for electronic transactions [7]. QIE refers to the qualification of all involved identities and the action taken upon data in the exchange between two or more persons. Multiple components are required for QIE, including electronic IDs (eIDs), data, processes, technical protocols and support. When it comes to eIDs, the eIDAS regulation (which is effective for all EU member states) introduces the notion of qualified trust service providers (QTSPs), indicating requirements and obligations that ensure high-level security of whatever qualified trust services and products are used or provided. The goal is to enhance in particular the trust of consumers and enterprises in the internal market and to promote the use of trust services and products. More on this in Section 6.1

Table 1 provides an overview of the prerequisites for QIE. The concept of an 'information game' is used to refer to formal interaction between two persons within a specified context. Here, the term 'person' refers to either natural person or a legal entity that can act as it were a natural person. Persons cooperating towards a specific goal have to exchange information in order to achieve the goal. There are numerous examples of such exchanges, for instance purchase orders from a web store towards a wholesaler. Or a pre-notification of the moment of arrival of a ship with a nuclear cargo towards the port authorities.

Table 1 suggest that QIE is only possible if participants know the identities, the context, the claims about information, and the position of each other in the game. These prerequisites are often specified — albeit in a more open and abstract way — in laws and regulations. Based on these prerequisites, the next section presents design guidelines for supporting these needs in an eSociety.

4 DESIGN GUIDELINES FOR QUALIFIED INFORMATION EXCHANGE

This section specifies design guidelines for an infrastructure that enables qualified information exchange. These are based on literature, legislation, and best practices, and would ideally all be met. We define an infrastructure as the complete set of technologies and organizations that work together under a formally defined set of agreements. The design guidelines are outlined in below.

(1) Effectivity [2, 17, 19]
   - enable persons to securely send and receive information, with a high degree of certainty about the identity of the sending and receiving person (prerequisite I).
   - enable persons to take position with respect to the formal submitting and accepting of information by means of a qualified signature (prerequisite IV).
   - enable persons to take position with respect to the formal submitting and accepting of information by means of a qualified signature (prerequisite IV).
   - enable persons to claim certain responsibility with respect to information by means of a qualified signature (prerequisite III).
   - enable persons to take note of any available information games (prerequisite II).

(2) Indisputability [14, 16]
   - allow transparency and traceability of positions taken in information exchange (than can be considered as the legal status) for a certain period of time (prerequisite IV).
   - allow positions taken in information exchange to be linked to a specific context (prerequisite II).

(3) Efficiency [5, 18]
   - enable submitting, accepting, securing and organizing qualified information at low costs (costs can be a barrier for adoption).
   - distribute the burden of providing trust (i.e. the provision of identities, authentication and authorisation) to the nodes instead of the core of the infrastructure.

(4) Openness [3, 4]
   - governed by an open system: allow involved parties to have a voice and insight in the construction, architecture and control of the common parts of the infrastructure.
   - fulfil a general utility. To ensure independence, creating and controlling these common parts of the infrastructure should have as limited economic importance as possible.

(5) Expandability [3, 5, 7, 11, 17]
   - support multiple forms of qualified information exchange within multiple contexts (prerequisite II).
   - enable persons to publish new contexts for new qualified information exchange games (prerequisite II).

(6) Control over personal data (privacy management) [1, 8, 19]
   - enable persons to have appropriate and exclusive control over information of which they have rights or have acquired rights within a specific context.
   - minimize (unnecessary) data accumulation and limit confidential data distribution.

(7) Reliability [3, 17]
   - perform according to predefined and agreed upon specifications.

(8) Compliance [3, 16]
   - facilitate and uphold information exchange that is lawful, i.e. be compliant with the relevant legal frameworks.
   - incorporate standards and agreements international standards (prerequisite II).

The design guidelines presented above were used to design the architecture presented in section six. First, section five takes a closer look at the challenges faced by Willeke when interacting with the Tax Office.

5 DIAGNOSIS: WHY WILLEKE STILL RECEIVES PAPER ENVELOPES

An existing case of qualified information exchange between persons that can act as a diagnosis example is the pre-completed income tax return (PCITR) of natural person Willeke, who, for her income tax submission, calls in the help of an intermediary, which is another person (a limited liability company) named BB Tax Ltd. BB Tax has access to an application which is connected to the standard business reporting (SBR) shared governance infrastructure over which the Tax Authority has made its services available in the Netherlands[3].

Table 1: Prerequisites for qualified information exchange based on the needs of persons to participate in it

Persons need to know the	*Description*	*Why is this necessary?*
I. Identities. Who are we interacting with?	Identities must be verified and it must be clear which formal role a person has in society and in the specific information game. The roles are determined by the type of person within a legal framework.	Knowledge about identities are necessary in order to determine if a person wants to enter a dialogue with the other. For some games, it may also be necessary to determine if the opposite person is some form of authority or is authorised (has permission) to enter the dialogue on behalf of someone else, for a specific purpose. In case of disputes, it must be clear which identities are involved.
II. Context: which information game am I participating in? What are the rules of the game?	Ex-ante clarity is needed about: • the context and purpose of the information game; • the information required; • the quality (e.g., scope, timeliness, format) of the required information; • the channel (how to submit or disclose information); • the sequence of steps in the information game (clear beginning and end); • processing: how the disclosed information will be processed; • the timeframe (from and until when?); • the potential consequences (of disclosing and not disclosing correctly or on time); • access: who will have access and under which conditions?	Based on the knowledge about purpose, required information (and information quality) flow and consequences, an actor can decide if it wishes to enter the dialogue. One of the basic principles of the protection of personal data in the General Data Protection Regulation is the purpose limitation principle. The purpose limitation principle consists of two elements: data must be collected for specified, explicit and legitimate purposes only (purpose specification); and. data must not be further processed in a way that is incompatible with those purposes (compatible use) [19]. Based on this principle and knowledge of the exchange context, the appropriate authorities/competent bodies can in case of irregularities or disputes determine if the information request was proportional given the purpose limitation.
III. Claims about information	Persons must be able to qualify information, i.e. create a signature and claim responsibility over the content.	The commitments each person takes regarding information within the game must be clear. Depending on the type of game (and the timebox for taking a position) an explicit expression of intent or volition might be needed in order proceed with the next step.
IV. The position of each other in the game	The position of the persons in a dialogue — whether or not they have signed and submitted, received, accepted and processed a message and have send a response, or whether it is a 'game master' who sets the rules for an information game — must be known to the involved persons in an irrefutable way.	Knowledge of the latest position of a person allows the other persons to proceed with their processes with legal certainty.

To be able use this infrastructure, BB Tax has acquired a digital service certificate which ensures authenticity and data integrity of messages. This certificate is created within PKIoverheid, the Dutch government system for public key infrastructure. Today, Willeke does not have such a certificate because it is difficult and expensive to acquire such a certificate and she is not able to use it. Over the SBR infrastructure, Tax Authority has enabled the possibility for a tax intermediary to get the PCITR of Willeke electronically and in a structured format. Figure 1 illustrates the processes. The five steps illustrated in Figure 1 are discussed next.

(1) First BB Tax sends, with some level of certainty, a claim that it is qualified to receive the PCTR from Willeke. This claim has been digitally signed using the service certificate of BB Tax.
(2) Next, the Tax Authority sends a letter to Willeke's only known authentic address, her postal mailing address. Guarantees for sending and delivering are covered by postal law. The letter from the Tax Authority contains a randomly generated authorization code.
(3) When Willeke received the letter, she transfers the authorization code to BB Tax in a method that has been agreed to by BB Tax.
(4) BB Tax requests to receive the PCITR with attached authorization code, signed using the company's service certificate.
(5) The tax authorities provide the PCITR to BB Tax.

Most of the assurances of qualified information exchange are met in this chain, although several points stand out. First, usage of postal services does not make the verification process very efficient (guideline 3), confidential (guideline 6), or trustworthy (guideline

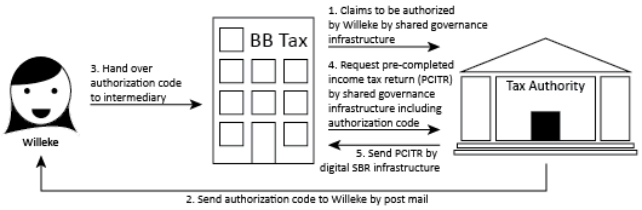

Figure 1: BB Tax, an intermediary, requests the pre-completed income tax return (PCITR) for Willeke from the Tax Authority over the SBR infrastructure

7). Willeke's housemates could open the mail. Or when Willeke claims to have never received the letter, it is impossible to trace what went wrong: did she lose the letter, or did she never receive it? Second, BB Tax uses an advanced, but not a qualified signature, which brings a lower level of assurance than if it was traceable to a natural person. Third, not the person who is responsible for her tax filing process (Willeke) is 'directing' the process, but the person who acts in behalf of this person (BB Tax). This does not enable Willeke to control her personal information (guideline 6): she does not know the content of the PCITR while she authorizes her intermediary to receive the PCITR on her behalf. Whenever a (formal) information process requires certainty about the identity and legal position, the process tends to rely heavily on postal services and their inherent disadvantages. The case described above, which is considered exemplary, endorses this claim. The act of signing documents in formal information processes also heavily relies on paper and wet signatures. Consider the examples listed in the introduction of this paper. Another particularly common example of this is signing of the authorization of automatic money transfers. Telephone companies, local parking authorities, and tax authorities still have processes in place which fully rely on paper. This is where paper enters the domain of business. As soon as a business executive acts within the context of his/her organization, more often than not, a wet signature is used. The barriers described are summarized in Table 2, related to the prerequisites for QIE specified in Section 3.

Standardization programmes such as SBR [3] have taken steps to specify the context of information games (prerequisite II), and the current paper focuses on the barriers in eSociety related to the other prerequisites. These barriers have in common that natural persons are currently lacking an electronic identity with a high level of assurance (in short: high-LoA eID) which they can easily apply within information games. Willeke still receives paper envelopes because she cannot yet digitally identify herself, register claims about information, and take position within information games in a trustworthy way.

6 ARCHITECTURE FOR QUALIFIED INFORMATION EXCHANGE

The previous section reveals that the most critical barriers for enabling QIE in eSociety come down to the limited availability of affordable and easy to use eIDs with the highest level of assurance (in short: high-LoA eIDs). Based on the developments that we see in the Dutch market of eIDs, we predict that within a few years, high-LoA eIDs will be commoditised. Assuming that this prediction is correct and persons like Willeke have a high-LoA eID, this section answers the question of what kind of infrastructure is needed for widespread QIE in eSociety.

Table 2: What are the barriers for an infrastructure for qualified information exchange in eSociety?

Actors need to know the	*What are the barriers?*
I. Identities	Natural persons are not "discoverable" digitally with the highest level of assurance. The Dutch government provides — in line with her mission statement in the 'Paper world' — digital authentication tools (password, password + sms) to its citizens with DigiD. The current issuing process takes place via post and has a substantial assurance level. The government does not provide and eID of the highest assurance level [13]. The eIDAS regulation does not regard digital identities embodied in email addresses, usernames and DigiD as qualified identities [7].
II. Context	There is limited access to a cross-community, easy to use and flexible approach for the specification of formal interactions (designing information games) as well as making rules of the game known for persons (understanding information games). Standardization programmes such as SBR are already taking steps to specify the context [3].
III. Claims about information	Natural persons have limited access to low threshold and affordable tools that enable them to use highly verified digital identities for placing qualified signatures and express volitation (intent) in a formal information game [20].
IV. The position of each other in the game	Natural persons have limited access to affordable and easy to use tools that enable them to rapidly submit and accept digital formal information.

6.1 Architecture based on three building blocks

As depicted in Figure 2, the proposed architecture builds on three main building blocks. As a starting point, each person has their personal data space (PDS), provided by a qualified trust service provider (QTSP). This establishes eIDs and related action possibilities for each person. Three main building blocks are required: (A) secure exchange between the PDS of each person, (B) coordination functionalities provided by the qualified ring, and (C) governance over this infrastructure. Each building block is explained below.

A **Qualified trust service provider (QTSP).** With Regulation EU No 910/2014 about electronic identification, authentication, and trust services for electronic transactions (eIDAS) in 2014, the European parliament has paved the way for a common electronic identity system for Europe. QTSPs are subject to the requirements of the eIDAS regulation, in

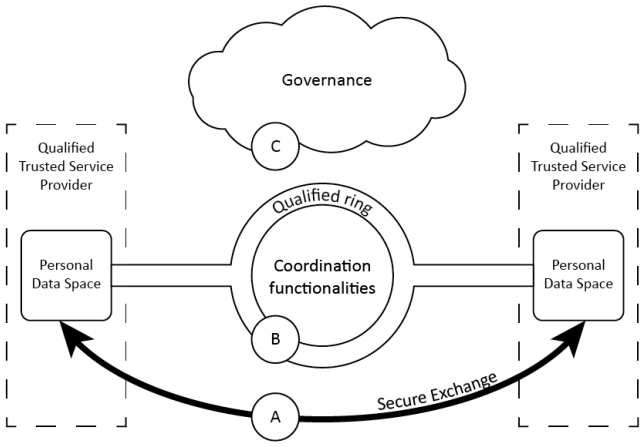

Figure 2: An architecture for qualified information exchange

particular those on security and liability to ensure due diligence, transparency and accountability of their operations and services. The starting point is that a QTSP, as defined within eIDAS, enables persons to act upon information with a high-LoA eID (prerequisite I). Actions include qualifying information with digital signatures (prerequisite III) and submitting and accepting information for a specific purpose (prerequisite IV). This creates for each person a personal data space (PDS) and enables secure exchange from one PDS directly to another.

B **Shared coordination functionalities.** To enable multiple QTSPs to interoperate in an open system (guideline 4) a limited set of coordination functionalities need to be facilitated as lean and secure as possible. We developed a prototype of such an infrastructure and use the working title 'qualified ring'. The qualified ring is tokenization system. Tokenization involves exchanging signed surrogates as pointers for real data that is securely stored in the edge systems — referring to the PDS of the end users. Based upon a person's action, such as submitting a message, the qualified ring enables the involved QTSPs to find each other and to establish a shared audit trail. Only tokens are sent over the qualified ring. Since content (the actual information that users want to submit) can be exchanged over direct (peer 2 peer) channels between QTSPs (building block A), this only needs to involve minimal notification data with limited business value in itself (guideline 4).

C **Shared governance.** Several decisions need to be made, enforced, and re-evaluated about the basic games and connectivity that this system enables. These decisions include: who can connect, what types of identities are recognised, how should an information dialogue be realized technically, and how can persons find each other. These decisions are made in shared governance over the qualified ring and over responsibilities for each participating QTSP (guidelines 4 and 7). The next sections explain how each of these building blocks is realized.

6.1.1 Secure exchange between trusted identities. Each natural and legal person can register an eID that has a high LoA within the eIDAS framework (prerequisite I). This eID is recorded in a set of X.509 certificates, the private keys of which are under exclusive control of the people who are allowed to act on behalf of the identified person. These certificates are issued by a QTSP that the person may select (guideline 7). In the Netherlands, several QTSPs are available within the public key infrastructure for the government, and currently support registering people and organisations based on evidence from several authentic sources, such as the municipal administration, the unique healthcare provider register, and the trade register. This system allows for interoperable identification and authentication of persons within various e-communities (guideline 5) using proven standards (guideline 1). In order to support qualified information exchange, the scope of the QTSP needs to be extended beyond only issuing proofs of identity (certificates). A QTSP must offer basic trusted functionalities that enable their users to act as a person in relation to information. By providing the eID along with these action possibilities, a QTSP offers each of its users a PDS which is coupled with one single identity of a natural or legal person. A PDS is uniquely linked to person and provides the essential functions for a person to participate in QIE with a High LoA EID. The essential functions (or action possibilities) are listed below:

- Importing and exporting information in open standard formats, which leads to data portability (guideline 7).
- Creating and verifying an advanced and qualified electronic signature to record accountability for information (guideline 1).
- As a special case of the previous functionality, create and interpret statements about the information games the person is willing to participate in (prerequisite II).
- Creating a qualified message: information that is disclosed by a submitter to a specific set of acceptors, within the context of an explicitly defined game, described in a standardised structured message format (prerequisites II and III).
- Submitting, accepting, and rejecting such a message, explicitly using a standardised notification format that secures integrity and non-repudiation (prerequisite IV).
- Accessing information created by the user or disclosed to the user with an accepted message, where the user must be authenticated using their eID (guideline 3).
- Archiving information and notifications for long-term validity independent of cryptographic advances, using RFC 3161 timestamps set by the QTSP (guidelines 1 and 2).
- Authorising other persons (such as a company's functionary or trusted person in the environment) using their own eID to perform any of these actions in name of the person, using standardised authorisation notifications (guideline 4).

We define personal data management as the exertion of these functions for the performance of qualified information exchange. Figure 3 provides an overview of how Willeke can use her High LoA EID which is linked to her personal data space.

Although the file formats and legal requirements must be standardised, in order to provide data portability (guideline 7) and assurance based on proven standards (guideline 1), multiple QTSPs may

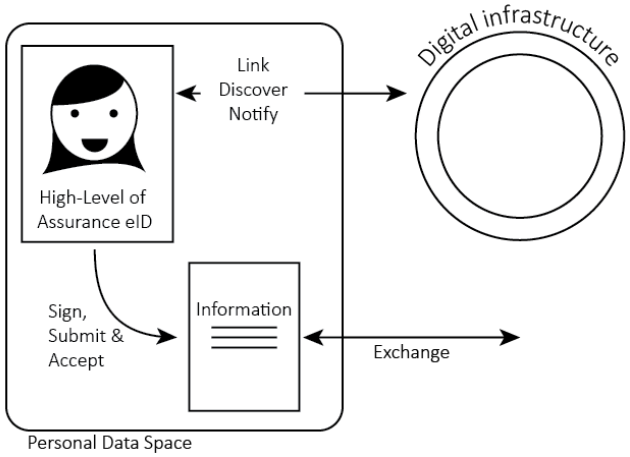

Figure 3: Personal data management: acting on personal data

offer these functions listed above in diverse ways (guideline 7). For example, one commercial QTSP might specialise on high-volume automated messaging with an easy-to-use REST protocol for information processing companies, while another QTSP specialises in a specific end-user interaction style or specialised authorisation structures, and a government-hosted QTSP provides basic functionality for all citizens. Since the QTSP manages integrity of information, this architecture allows for qualified derived claims (e.g. linking attributes to pseudonyms or creating derived reports with the minimum of information for a particular purpose) (guideline 6).

6.1.2 A qualified ring for coordination functionalities. To enable multiple QTSPs to interoperate in a distributed and open system, these need to have access to a shared set of coordination functionalities. Essential coordination functionalities include:

- Identifiers and addressing. To share the position a person takes with regard to information (e.g. the person submits information), the person's QTSP sends a notification over HTTPS using a central URL of the qualified ring. This notification contains identifiers for the audience of the notification, which the qualified ring uses to notify the audience's QTSPs. This routing architecture enables any person to reach any other person by just knowing the identifier, without knowing the technical address of the other person's data space or QTSP. A tree structure of namespaces is registered in order to have an open system of such identifiers (guideline 4). For example, Dutch government organisations can be identified uniquely using their organisation identification number, while private companies can be identified using their trade register number. QTSP-specific namespaces enable persons to register multiple addresses leading to a single eID, which allows for pseudonyms and cross-domain usage of a single eID: while different submitters may know different names for an acceptant, the acceptant can manage incoming message in a single personal data space.
- Notifications and an audit trail. Message-related notifications created by a person (submitting, accepting, or rejecting a qualified message) and notifications created by a QTSP (delivery of information content, or errors) are stored centrally, for long enough time to ensure delivery even in the case of temporary QTSP downtime. Only a QTSP currently registered for a person can access notifications relevant to that person over a secure channel (guideline 6). These notifications are digitally signed and contain cryptographic hashes over the exchanged information and over previous notifications, which turns them into a shared integrity-checked audit trail (guideline 2).

The qualified ring serves general interests of QTSPs and the persons they serve, and it must be impartial. The coordination functionalities and the information involved have limited business value in itself (guideline 4). In order to provide sufficient notification functionality and an audit trail, no information other than identifiers and sufficient cryptographic hashes and digital signatures need to be processed by the qualified ring itself. Once two QTSPs are authorized to deliver and retrieve information content, they do so over a direct connection that does not involve the qualified ring.

6.1.3 Governance: public-private collaboration. The described system, distributed between QTSPs and the qualified ring, only works if the involved parties share a system of agreements. These include agreements on questions such as the following. Under what conditions is a QTSP allowed to connect to the qualified ring, and how is supervision upon these conditions managed? What types of identities are recognised? What entities are acknowledged as natural or legal persons, and what relevant (professional) qualifications can be attributed to them? How should an information dialogue be realized technically, and what legal assurance does each step in this dialogue bring? I.e. if one person receives a notification of another, what legal meaning does it have? How can persons find each other? These decisions are made in shared, democratic governance over the qualified ring and over responsibilities for each participating QTSP (guideline 4). Members of the governance organisation should represent persons that have a significant role as a submitter, acceptor, or game master.

7 EVALUATION OF THE PROTOTYPE

The previous section introduced a design for realising qualified information exchange in an eSociety. In this section we evaluate the use of the qualified ring with two prototyped user stories. These concern two information games: a simple game where little specification is needed, and a more composed game that is composed of multiple instances of this basic game. The prototypes are evaluated from the viewpoint of Willeke.

7.1 User Stories

7.1.1 Willeke wants to confirm an agreement with her advisor. After starting a sole proprietorship, Willeke's personal income tax has become more complicated and she wants the assistance of a tax advisor. She has received a quotation from tax advisor BB Tax and wishes to return it with her confirmation that the contract may start. While today this would involve some paperwork and a wet signature, in this scenario both Willeke and BB Tax have a personal data space (PDS) connected to the qualified ring. The quotation is a PDF document containing a qualified signature created by one of

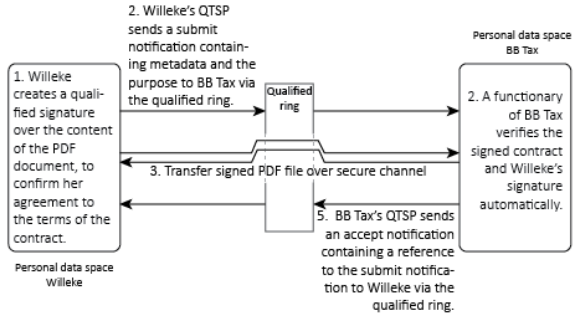

Figure 4: Willeke shares a signed PDF file with BB Tax

BB Tax' directors. This quotation is uploaded to Willeke's PDS. To confirm, Willeke needs to return a version of the same document that is signed using her own citizen certificate. Willeke can share the signed contract with BB Tax in a basic game, where each person can take a position related to the contract: Willeke becomes the submitter and BB Tax becomes the acceptor. These positions are captured in a notification: metadata sent over the qualified ring. The content of the contract itself (the signed PDF file) is not sent over the qualified ring, but directly from Willeke's PDS (hosted by a QTSP of her choice) to the PDS of BB Tax (hosted by a QTSP of their choice). Looking more closely at this basic game, the following steps can be distilled (Figure 4). The five steps followed in Figure 4 are explained next.

(1) Willeke creates a qualified signature over the content of the PDF document, confirming her agreement to the terms of the contract. As a result, her PDS contains a signed copy of the document. This satisfies prerequisite III: Willeke has claimed responsibility over the content she is going to share.
(2) Upon Willeke's initiative, Willeke's QTSP sends a submit notification to qualified ring. This notification contains the metadata required for BB Tax to retrieve and verify integrity of the PDF file from Willeke. It also specifies the purpose of "confirming an agreement".
(3) Upon receiving the notification, the QTSP of BB Tax opens a secure connection with the QTSP of Willeke to transfer the signed PDF file.
(4) Now a functionary of BB Tax verifies the signed contract and Willeke's signature. The QTSP of BB Tax could offer automated pre-processing as a service: it verifies whether the quotation has expired, verifies whether the PDF content is unchanged since BB Tax first shared it, and verifies whether Willeke's signature is expected and valid.
(5) Upon the initiative of the functionary of BB Tax, its QTSP sends an accept notification to qualified ring. This notification contains a reference to the submit notification and a cryptographic hash over its content and is protected both by the functionary's qualified signature and by a qualified timestamp created by the QTSP of BB Tax. It is addressed to Willeke using the identifier from the submit notification. The accept notification serves two goals: the PDS of Willeke is notified of the message status update, and BB Tax takes position as an accept of the message (prerequisite IV).

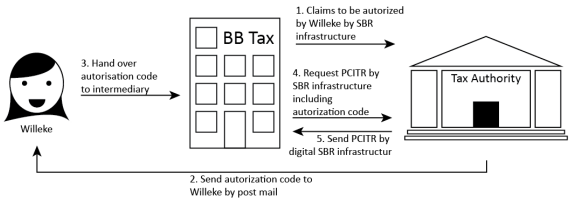

Figure 5: Composed interaction for the 'pre-completed income tax return' case

To support this basic information game for Willeke, the PDS should make it easy for her to import and export documents, to sign them, and to submit them. This basic game provides sufficient notification types to satisfy the positions persons take: submit and accept. For situations with less trust between submitter and acceptor, the game could be extended intermediate steps and notification types. For example, the QTSP may issue a "delivery notification"right after transferring the file, confirming when exactly BB Tax had the content at its disposal. For additional security, the acceptor may be required to take more intermediate positions before getting access to the content of the message: agreeing to receive a message, agreeing to metadata such as the purpose limitation of the message, and finally accepting the message after receiving the content.

The same steps can be followed to sign any type of agreement in a low-threshold way. This can for example cover a lot of cases in the HR domain, where currently often physical appearance and wet signatures are involved. Note that the message purpose ("confirming an agreement") in the example is generic and imposes no specific restrictions upon the scope in which its information may be further disclosed or processed. Such restrictions can be stated in the contents of the agreement, or in a terms and conditions document that it refers to, but this requires people to read the terms which limits the ways in which these dialogues can be automated.

7.1.2 Willeke wants her tax advisor to complete her income tax return. The next example shows a game with a more elaborate specification, based on the pre-completed income tax return (PCITR) case in Section 5 (Figure 1).

Basically, this game contains a chain of simple interactions like the one described above. However, since in this game the purpose of each step is specified, several steps can be performed automatically or be made easy by a user interface. Now that Willeke has reached an agreement with BB Tax for completing her income tax return, BB Tax needs to have Willeke's PCITR. Since Willeke now has direct access to qualified ring with a verified and trusted identity, BB Tax does not need to act as her representative as it did in Figure 4. The interaction happens in three phases (Figure 5), each of which is composed of a variation on the basic game presented in Section 5. The three steps illustrated in Figure 5 are explained next.

(1) Willeke submits a request for her PCITR to the Tax Office. She can do so using her own citizen certificate, containing her social security number, which is known to the Tax Office. This submission follows all steps from the previous example, but in this case the message content is more standardized (e.g. a signed request message conforming to a published

specification) and the purpose is defined more specifically: "requesting my PCITR". As a result, the Tax Office prepares the PCITR.

(2) Since the Tax Authority now has an address for Willeke, it can submit the PCITR directly to her. Again, this is a simple submission, with a standard message content (e.g. an XBRL instance) and a specific purpose: "providing a personal PCITR".

(3) After Willeke receives the form in her PDS, she forwards it to BB Tax. As a company that provides tax advice services, BB Tax is an authorized acceptor for this type of message. This is again a simple submission, with the same message content and a specific purpose: "completing the PCITR as part of the agreement". By accepting this message, BB Tax confirms that this request can be fulfilled as part of the agreement between Willeke and BB Tax.

Note that most of these may not need Willeke's active involvement: as a service, her QTSP may offer to request, accept, and forward the form at an appropriate time each year. In order for this three-phase game to work, it is essential that all participants agree on the legal consequences of each position and step. Therefore, the game needs to be governed and specified precisely by a delegation that might include the Tax Authority itself and the Dutch Association of Tax Advisors. Similarly, interest groups in other domains may specify multiple-step games in these domains.

7.2 Prototypes

Together with a QTSP, working prototypes have been realised for the qualified ring and the required personal data space functionalities. Note that all relevant technology, such as electronic signature creation and validation, is well known and open source implementations exist. The prototype assumes that high-level-of-assurance identities for citizens and organisations are available at low cost and in a way that is easy to use. In the Netherlands, at least one QTSP is currently available that provides these identities in a way that has proven to be compliant to eIDAS and PKIoverheid norms. The regulation on eIDAS is technology neutral. Over time, we have considered a range of technologies as part of the prototype, including X.509, SSL/TLS, SAML 2.0, OpenID, Oauth, PKCS#, S/MIME, XML-DSig, XAdES, PAdES, CAdES, WS-*, etc.

For the paper discussing the prototype in this we refrain from discussing detailed technical specifications. Instead, we explicitly focus on the interaction between QTSP and the Ring. This QTSP enables citizens to register eIDs for themselves and their organisations remotely by phone (reducing registration costs) and to control a cloud-based qualified electronic signature creation device using the same phone (enabling an easy-to-use interface). It is expected that more QTSPs will follow, including a basic one for general use by the government. The goal of the setup was to enable a basic information exchange game (submit and accept information between two trusted identities) and a complex game (submit a PCITR in a standard format to a validation service, then send it to the tax authorities). The setup for evaluating the prototype:

- A natural person with a Dutch passport and a Samsung Galaxy S7 smartphone. Mobile devices have become the something-you-have authentication factor that has been generally delegated to hardware tokens. Smartphones allow deploying highly-secure yet user-friendly mechanisms that can complement existing national eIDs and overcome user-experience drawbacks.
- A working QTSP certification service for natural persons fully accessible using a smartphone app
- A qualified electronic signature creation application, accessible by smartphone
- A server running the prototyped qualified ring infrastructure
- A server and user interface for additional QTSP functionalities, based on X.509 certificates such as the ones originating from the QTSP certification service

The next sections explain how and to which extend each of the building blocks of Section 6 are realized in the prototype. It takes less than 15 minutes for a natural person to acquire their digital identity from the QTSP. The digital authentication and signing certificate can be used subsequently in the qualified information exchange prototype. For the prototype of secure exchange between trusted identities, two types of PDS interfaces (one user interface, one automated API) for trusted identities have been build. The first are the PDSs for natural and legal persons with a user interface to manually import data and submit messages. The second is an automated PDS for a data service provider that validates and signs PCITR documents. The natural and legal persons have a personal data space in which they can import and export documents, create and verify electronic signatures with their certificate, create qualified signed message notifications and submit and accept these. Each message is signed with the user's qualified signature to create a record of accountability. The information itself can be accessed through a secure REST interface between QTSPs, where access is validated using the certificate of user that created the information, or the user the information was disclosed to. Messages and notifications are stored securely by the QTSP, time stamped and identifiable by the cryptographic hash over their content, ensuring data integrity.

The data service provider (i.e. BB Tax) can automatically process and sign the PCITR document, using the same principles as any other trusted identity on the qualified ring. This means it can automatically accept notifications, validate documents, submit notifications about the result and disclose the validation results to a specified audience. QTPSs and data service providers can connect to an open system to address each other by their ID. They can send notifications over a central REST interface to the qualified ring. These notifications contain the identifiers for the audience of that message. Based on this notification, the qualified ring is able to notify all audience QTSPs, so they can retrieve the notifications. A first design of the governance model shows that the ring will be governed by a non-profit foundation with members from a number of involved public and private parties. The operational and organisational costs will be covered by QTSPs and qualified service providers based on the number of messages send over the ring. All financial, operational and technical decisions are open to all members. A prototype website is built to publish these first set of rules.

7.3 Can this help Willeke?

Let us consider the extent to which the proposed solution could help Willeke to achieve her goals. Willeke wants:

- to confirm an agreement with her tax advisor. Using the proposed solution, Willeke can submit and accept information securely and irrefutably to any person that she knows with an eID and a PDS.
- her tax advisor to complete her income tax return. Using the proposed solution, Willeke can send her PCITR via an automated processing service to a tax authority that is connected to the ring.

The prototype enables Willeke to fulfil her goals, but also shows the potential to perform many more comparable basic information exchange games. It also shows that the possibility to perform complex games is not limited by technology. The most important innovation still needed for these complex games is in governance: organisations must specify precisely the information games they partake in, and the positions that persons can take regarding information within these games.

8 CONCLUSION

This paper started by asking when Willeke can get rid of paperwork. Our answer is: as soon as she has access to a affordable and easy to use high level of assurance electronic identity and the functions required for personal data management within relevant legal frameworks. We have demonstrated this within the eIDAS framework with a design for a network of qualified trust service providers (QTSPs). These QTSPs enable their users to register a qualified identity, do claims about information, and take position in information games. To ensure that this system can be widely accepted, the shared coordination functionalities are designed to process minimal information of business value. We argue that such an infrastructure should be steered by a public-private governance. The success factor for helping Willeke lies in our ability to get public and private organisations to work together in a public-private governance in which actors are committed to facilitate information games via the proposed solution.

9 DISCUSSION

There are a couple of limitations to this study. First, in our prototypes, we did not specify authorisations between persons. We believe that we can use the same method of notifying as used in other information exchange. We have not yet prototyped this solution. Second, this study does not address challenges for migrating from existing implementations for (qualified) information exchange to the presented solution. We expect that it is key to start with basic games that have high value for early adopters like Willeke, such as signing, submitting and accepting digital contracts. Third, we did not perform a comparative study on various technologies that can be used within the proposed architecture. We do not claim that the architecture proposed in this paper cannot be realised with other technologies.

We consider this study to be a first step to free Willeke of paperwork. A lot still needs to be done. Given that policy makers are currently looking for solutions that enable personal data management for individuals like Willeke, we anticipate that our future work will focus on testing the solution proposed by this paper with a small number of public and private organizations.

REFERENCES

[1] Luca Belli, Molly Schwartz, and Luiza Louzada. 2017. Selling your soul while negotiating the conditions: from notice and consent to data control by design. *Health and Technology* 7, 4 (dec 2017), 453–467. https://doi.org/10.1007/s12553-017-0185-3

[2] J. Bender. 2016. eIDAS Regulation: eID - Opportunities and Risks. (2016).

[3] N. Bharosa, R. Van Wijk, N. De Winne, and M.F.W.H.A. Janssen. 2015. *Challenging the Chain: Governing the Automated Exchange and Processing of Business Information.* Delft University Press, Delft. https://doi.org/10.3233/978-1-61499-497-8-i

[4] S Davidson, P De Filippi, and J Potts. 2016. Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology. (2016).

[5] Zakareya Ebrahim and Zahir Irani. 2005. EâĂŘgovernment adoption: architecture and barriers. *Business Process Management Journal* 11, 5 (oct 2005), 589–611. https://doi.org/10.1108/14637150510619902

[6] EIDAS. 2014. EU regulation no 910/2014 of the European parliament and of the Council of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. (2014).

[7] Patrick Genoud, Giorgio Pauletto, and Jean-Marie Leclerc. 2004. The e-society repository: Transforming e-government strategy into action. In *4th European Conference on E-government, Dublin Castle, Ireland.* 17–18.

[8] Stefania Gnesi, Ilaria Matteucci, Corrado Moiso, Paolo Mori, Marinella Petrocchi, and Michele Vescovi. 2014. My Data, Your Data, Our Data: Managing Privacy Preferences in Multiple Subjects Personal Data. Vol. 8450 LNCS. Springer Verlag, 154–171. https://doi.org/10.1007/978-3-319-06749-0_11

[9] Alan R. Hevner, By Salvatore T March, Jinsoo Park, and Sudha Ram. 2008. Design science in information systems research. *MIS Quaterly* 32, 4 (mar 2008), 725–730.

[10] ITU. 2017. *Measuring the Information Society.* Technical Report.

[11] S. Jayashree and G. Marthandan. 2010. Government to E-government to E-society. 10, 19 (2010), 2205–2210.

[12] H Kruger, L Drevin, and T Steyn. 2007. Email Security Awareness âĂŤ a Practical Assessment of Employee Behaviour. In *IFTP International Federation for Information Processing, Volume 237, Fifth World Conference on Information Security Education*, L Futcher and R Dodge (Eds.). Springer, Boston, 33–40.

[13] Ministry of the Interior and Kingdom Relations. 2012. eID stelsel Nederland: Strategische verkenning en voorstel voor vervolg (in Dutch). (2012).

[14] Masakazu Ohashi and Mayumi Hori. 2010. Certified Originality of Digital Contents by the Time Authentication. In *Information Communication Technology Law, Protection and Access Rights.* IGI Global, 67–80. https://doi.org/10.4018/978-1-61520-975-0.ch005

[15] Ken Peffers, Tuure Tuunanen, Marcus A. Rothenberger, and Samir Chatterjee. 2007. A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems* 24, 3 (dec 2007), 45–77. https://doi.org/10.2753/MIS0742-1222240302

[16] Sélinde van Engelenburg, Marijn Janssen, and Bram Klievink. 2017. Design of a software architecture supporting business-to-government information sharing to improve public safety and security. *Journal of Intelligent Information Systems* (jul 2017), 1–24. https://doi.org/10.1007/s10844-017-0478-z

[17] R. Van Wijk, S. Bal, N. De Winne, and J.P. Van Der Woerd. 2016. *Qualified Information Exchange: 21st Century Business Reporting.* Big Bites Publishers, The Hague.

[18] Viswanath Venkatesh and Hillol Bala. 2012. Adoption and Impacts of Interorganizational Business Process Standards: Role of Partnering Synergy. *Information Systems Research* 23, 4 (dec 2012), 1131–1157. https://doi.org/10.1287/isre.1110.0404

[19] Paul Voigt and Axel von dem Bussche. 2017. *The Eu General Data Protection Regulation (gdpr): A Practical Guide.* Springer.

[20] World Economic Forum. 2016. *A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity.* Technical Report.