Co-Creating Requirements for the Emerging Electronic Identity Management Platform

Bakhaev Stepan, Naqvi Bilal, Wolff Annika, Smolander Kari

9-22-2023

CO-CREATING REQUIREMENTS FOR THE EMERGING ELECTRONIC IDENTITY MANAGEMENT PLATFORM

Stepan Bakhaev
Lappeenranta-Lahti University of Technology, stepan.bakhaev@lut.fi

Bilal Naqvi
Lappeenranta-Lahti University of Technology, syed.naqvi@lut.fi

Annika Wolff
Lappeenranta-Lahti University of Technology, annika.wolff@lut.fi

Kari Smolander
Lappeenranta-Lahti University of Technology, kari.smolander@lut.fi

CO-CREATING REQUIREMENTS FOR THE EMERGING ELECTRONIC IDENTITY MANAGEMENT PLATFORM

Research paper

Bakhaev, Stepan, Lappeenranta-Lahti University of Technology, Software Engineering, Lappeenranta, Finland, stepan.bakhaev@lut.fi

Naqvi, Bilal, Lappeenranta-Lahti University of Technology, Software Engineering, Lappeenranta, Finland, syed.naqvi@lut.fi

Wolff, Annika, Lappeenranta-Lahti University of Technology, Software Engineering, Lappeenranta, Finland, annika.wolff@lut.fi

Smolander, Kari, Lappeenranta-Lahti University of Technology, Software Engineering, Lappeenranta, Finland, kari.smolander@lut.fi

Abstract

Digital transformation of public sector entails prominence to electronic identity (e-ID) management platforms. The new, user-centric systems for e-ID management can be enhanced with Artificial intelligence (AI) and distributed ledger technology (DLT). However, such technological complexity can make these systems counter-intuitive for an ordinary user. Existing research identifies that the socio-technical arrangements for e-ID platforms are often ignored. In this study, we investigate what kind of requirements users have for an e-ID management platform in public sector. We employed principles of co-creation methodology to design and run a series of workshops in five European municipalities. Despite technological propositions of an e-ID platform, accessibility, usability, and security attributes were the most debated issues among the prospective users. The results from the co-creative requirements elicitation suggest for broadening the discussions around e-ID management platforms to encompass social and socio-technical aspects in the design and development of these systems.

Keywords: Digital Platforms, Electronic Identity, Co-creation, Public Sector

1 Introduction

Digital technologies offer new opportunities and push for alternative models of government (OECD, 2020). A substantial transition of public services to online format puts electronic identity (e-ID) management at the core of emerging platforms enabling interaction between citizens and their governments in a new landscape (Söderström, 2016; Bazarhanova, 2020).

The developments in artificial intelligence (AI) have been drawing attention of public organizations seeking to reduce their administrative workloads and serve citizens in more efficient and accessible ways (Alexopoulos *et al.*, 2019; Floridi, 2020; Drobotowicz, Kauppinen and Kujala, 2021). For electronic identification, AI algorithms provide with sophisticated methods for corroborating human-user's identity, such as image processing and biometrics, including facial recognition. However, the ethical concerns of AI application in organizational contexts such as data privacy, automation and bias, increased the awareness of associated challenges for users' trust (Berente *et al.*, 2021; Holmström and Hällgren, 2021; Lockey *et al.*, 2021).

A distributed ledger technology (DLT) holds a premise in alleviating the trust issue by decentralizing communications and distributing decision-making through cryptographically secured peer-to-peer networks (Lindman, Tuunainen and Rossi, 2017; Vergne, 2020). The infrastructures built upon DLT, such

as blockchain, potentially advance e-ID management with the Self-Sovereign Identity (SSI) principle which would allow users to control and selectively disclose their information essential for identification (van Bokkem *et al.*, 2019; Liu *et al.*, 2020; Vergne, 2020). Software-based systems designed around this principle and enhanced with biometric authentication can enable a truly user-centric model of identity management in public sector.

However, the subtle nature of decentralized e-ID platforms emerging from the novel technologies can hamper the non-technical users' understanding of the core processes in (personal) identity management (Whitley, Gal and Kjaergaard, 2014; Fridgen *et al.*, 2018). The security mechanisms based on cryptographic solutions are too complicated, and the underlying policies, such as user-managed data control, are too abstract making these systems unintuitive to a wider population (Whitten and Tygar, 1999). Given the dominance of a technical discourse on identity management (Čučko and Turkanović, 2021), the authors find problematic that the user-centric e-ID platforms are rarely driven by a user perspective despite calls for contextual views of their design (Melin, Axelsson and Söderström, 2016; Dunphy, Garratt and Petitcolas, 2018; Giannopoulou and Wang, 2021). That is, understanding the social and socio-technical arrangements of e-ID management in public sector can help communicate the requirements for solutions that meet the needs and interests of their users.

We therefore formulate the following research question: *what kind of requirements users have for the e-ID management platform in public sector?* The study we describe was situated in the context of large collaborative research project focused on the development of e-ID system for online public services. Our approach to requirements elicitation was inspired by co-creation as a methodology for engaging diverse stakeholders in participatory design practices (Sanders and Stappers, 2008). We designed a replicable workshop template and carried five separate sessions with prospective e-ID users from different European municipalities. Our findings, as empirical evidence from the workshops, suggest quality attributes pertaining to the e-ID systems' design from the user perspective. They also give prominence to non-technical factors for e-ID management platforms based on self-sovereign identity model.

The remainder of this paper is organized as follows. Section 2 describes related research. Section 3 introduces the study settings. Section 4 describes our methodology. Section 5 presents findings from the workshops. Section 6 discusses implications from the results. Finally, Section 7 ends the paper with short conclusion.

2 Related research

The user-centred design (UCD) approach to system development is employed for problem-solving focusing on user needs (Iivari and Iivari, 2011). One of the related challenges is that during the development phases users may not be able to communicate precisely or technically some requirement or other. However, they still can explain their goals and how they approach their tasks (Kujala, 2003). The contexts in which user-centred systems will be deployed are best understood by users themselves where they are considered the experts (Gulliksen *et al.*, 2003). Therefore, users should not be seen only as passive informants as they may have different values in relation to a system and its use (Kujala, 2008).

In design research and practice (see Figure 1), UCD relies on research-led practices primarily with an expert mindset to collect, analyze, and interpret data, in order to develop specifications and evaluate prototypes with specific tools and methods (Sanders, 2008). Conversely, co-creative mindset enables a participatory approach aimed for actively involving the people who are being served by design in the process of problem-solving (Sanders and Stappers, 2008).

As diverse as the user participation in public service design can be (Holgersson and Karlsson, 2014), the co-creation gained traction in projects addressing complex societal problems with user-driven ideas (Lee *et al.*, 2018; Trischler, Dietrich and Rundle-Thiele, 2019). Described as a continuation of participatory design originated in the Nordic region (Sanders and Stappers, 2012), this paradigm shift implies changing the roles of the researcher from 'translator' between the users and technologists to 'facilitator' of collaborative and creative design practices.

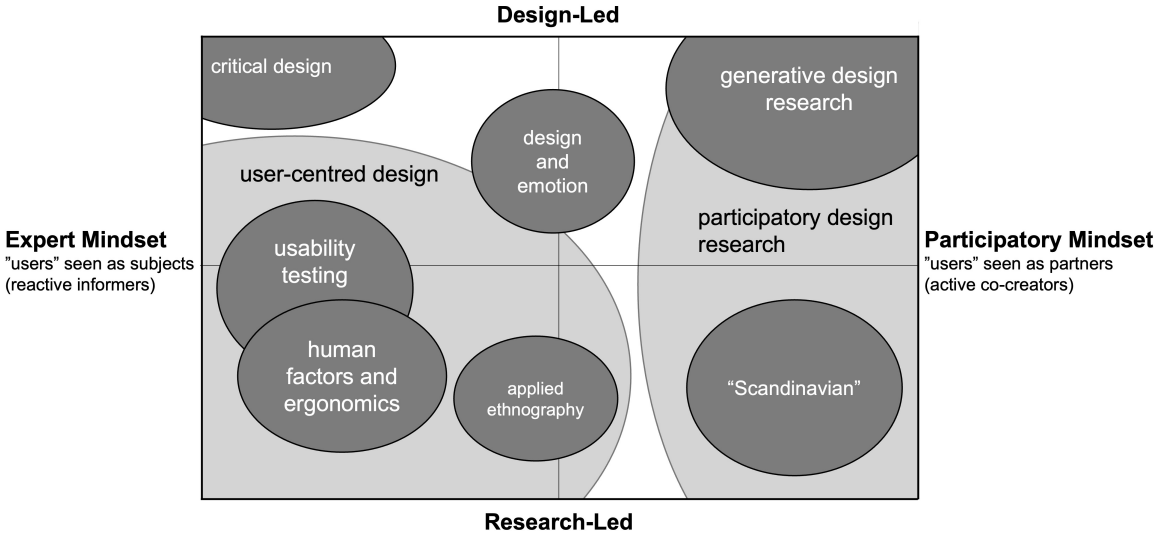

Figure 1. Design practice and design research map (Sanders and Stappers, 2008).

Different contexts of co-creation in design assessed by Jones (2018) are prompt for drawing on the key principles in applying it to the user-centred systems development:

- *Co-creation for dialogue*. In the view of value co-creation, it is both an organizing activity and a product of meaningful interactions that help to engage different stakeholders to explore their problems and experience desirable values.
- *Co-creation for design*. As a design methodology, it is a creative participatory practice that facilitates and informs collaboration between people of different knowledge and skills in articulating their ideas for problem-solving.
- *Co-creation for process*. As a structured approach to discussion, it allows the participants to continuously move from sense-making (i.e., understanding, and articulating stakeholder needs for design decision); to change-making (i.e., directing design decisions towards social or organizational change); and to "strange-making" (i.e., presenting typical design artefacts as original solutions).

In service design and research, the dialogical nature of value co-creation is realized through interaction between service providers and service users (Tuunanen *et al.*, 2019). Conceptually, it is the interplay of system value propositions and customer (user) value drivers as shown in Figure 2.

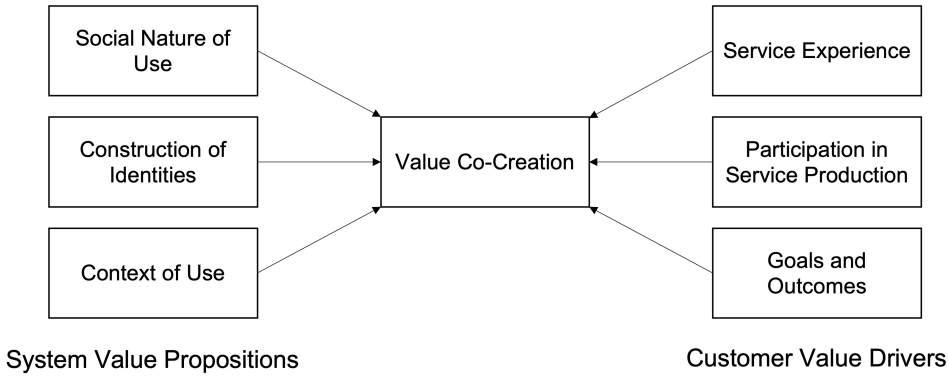

Figure 2. Value co-creation for services (Tuunanen, Myers and Cassab, 2010).

Discussing the expectations from e-ID management in public sector, Seltsikas and O'Keefe (2010) reflected the interplay of e-ID-enabled services and outcomes on the concepts of trust and public value. Their delivery was coupled with the transaction convenience of online services that provide trustworthy applications for public institutions. Further, Melin, Axelsson and Söderström (2016) stressed the user

perceptions of e-ID intertwined with the use of digital public services observing the challenges for e-ID development from a system life-cycle perspective. In light of digital government platforms, van Dijck and Jacobs (2020) argued that as a socio-technical construct "e-ID promotes public values such as privacy, identity control, security, and user empowerment". These values resonate with key propositions of the SSI principle (Allen, 2016), prompting their uptake in the technical frameworks of decentralized e-ID platforms (European Commission, 2021).

Still, there is a lack of work from both practitioners and researchers on design principles and requirements for the user-centred e-ID management solutions (Laatikainen *et al.*, 2021). This study therefore attempts to approach the requirements elicitation with the co-creation methodology. To explore user needs and concerns for e-ID management and how these may vary contextually, we aimed to engage public sector stakeholders from different case sites which we describe in the following section.

3 Study settings

The study was set within the European research initiative focused on the emerging digital platform for electronic identification of individual citizens and legal entities in accessing online public services. The proposed e-ID system is based on the SSI-model utilizing facial recognition and ID document verification for creating (onboarding) and managing user's verifiable credentials in a distributed ledger (blockchain) from their mobile device. To evaluate the solution, it is being deployed in multiple pilot sites coordinated by the partnering public administrations from the respective European countries. Each site provides unique testing environment formed by various factors, such as demographics of target users, featured public service, or maturity of prior e-ID schemes and digital government infrastructures. The case sites selected for study are outlined in Table 1, followed by their detailed description.

Case site	Public service	Target users
City of Aarhus, Denmark	Personal documents storage in lockers	Vulnerable citizens (homeless people)
Ertzaintza, Basque Country, Spain	Filing crime complaints via police web-portal	General public, police officers
City of Gijón, Spain	Municipal public services available in the city web-application	General public
Peshtera municipality, Bulgaria	Public services of e-government agency	General public
Italian Union of Chambers of Commerce (Unioncamere)	Digital business register for the enterprise entities	Entrepreneurs and legal representatives of small companies

Table 1. Overview of the study cases.

The *City of Aarhus* is set to provide shared lockers for personal documents storage. The lockers to be installed inside the municipal facilities, however only accessible with the cards containing a printed list of one-time codes for their opening, as the current solution for identification. The case owners see vulnerable citizens living in shelters as primary users of these lockers since they are usually exposed to lose their personal documents along with the code cards. Therefore, they aim to improve lockers' accessibility with the help of novel e-ID technologies.

The *Ertzaintza police* are exploring the prospects of e-ID technologies for online services, such as filing crime complaints through their web-portal. Currently, this service is implemented through a hybrid process, where complaints are registered online without prior authentication of a citizen. This requires the citizen to verify their identity physically at the police station within 72 hours to initiate investigation. The case owners anticipate streamlining their operational workflows as digitalization of public services evolves on a national scale.

Another Spanish municipality, the *City of Gijón*, features public services available to the residents holding a physical and non-transferrable "Citizen Card". The public administration considers the card as a recognized *de facto* identity document for the residents of their municipality. However, accessing public

services online, along with the card issuance via city web-application requires new means for citizens' authentication to facilitate their experiences.

The Bulgarian municipality of *Peshtera* presents a full list of the public services available on their own website. These services are provided by the state e-government agency and require citizen's authentication with a personal qualified electronic signature (QES). The process of obtaining QES for individual citizen is too cumbersome and is a subject to fee, making this option for e-ID unattractive for many. The case owners assume that the poor usability of QES results in low overall adoption of digital services for public sector, a situation they seek to improve with alternative e-ID solutions.

Finally, the Italian *Unioncamere* features another unique case site dealing with the digital services for entrepreneurs and business entities. These services are offered via web-portal operated by the national authorities. While prior Italian e-ID scheme allows company representatives for online authentication, the case owners consider potentials of DLT integration with the national business register.

4 Methodology

The study proceeded as exploratory research (Runeson and Höst, 2009). The heterogeneous and geographically dispersed case sites present challenges, as well as opportunities for experimenting with non-trivial techniques to elicit requirements for a common e-ID platform. To answer the research question, a co-creation workshop was designed and replicated in a series of five distinct sessions with the end-users from the respective locations. The workshops' results were collected and qualitatively analyzed in a cross-case comparison for deriving the concepts. To identify the kinds of requirements, the results were categorized in terms of the software quality model from ISO 25010 (2011). Figure 3 visualizes the research process followed in this study.

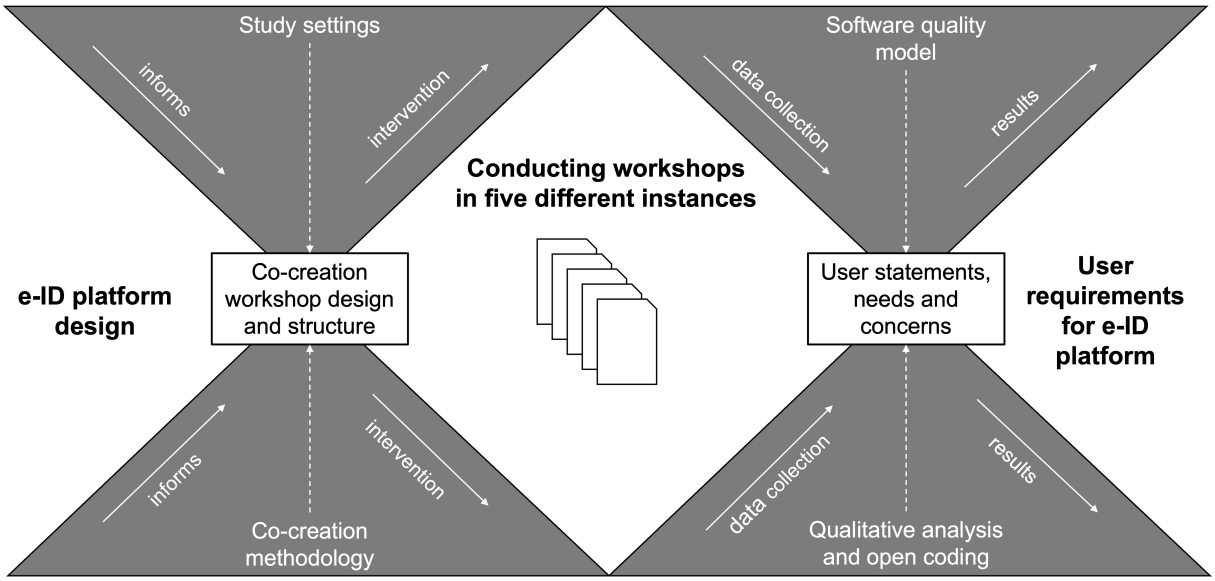

Figure 3. The research process.

4.1 Workshop structure

Assuming the remote conditions of partnering organizations, the workshop template was made adaptable to both physical (face-to-face) and virtual conditions employing online collaboration tools such as digital whiteboard and video-conference communication. It allowed the participants to collaborate, generate and discuss their ideas as they completed the following exercises.

At the beginning, the participants were introduced to the research context. The workshop facilitators conveyed the goals and vision of the project in a broad *"What? How? Why?"* outline describing the proposed e-ID platform. The facilitators further explained the expected outcomes of the co-creative

sessions reflecting in important ways the specifics of their study cases. Following the opening presentations, the participants were shown a demo video of the user onboarding the e-ID platform in the system's prototype. The purpose of this demonstration was to provide with tangible idea about e-ID technologies, envisioning interfaces and preparing for interactions in everyday use.

Step 1. The Positives. The first step was set to explore the positive user expectations from the proposed e-ID management platform. This was mainly a warm-up exercise designed for engaging a creative attitude and acclimating participants to the workshop format. In virtual settings, the exercise helped participants adapt to the interface of the digital whiteboard. In a short time (up to 10 mins), all participants had to write their statements, one per sticky note. Online, they could share their ideas and assumptions anonymously, but in either case (online or in-person), they posted notes without further comments to enable an open-minded, brainstorming environment. Once time was up and participants finished their writings, the first step was complete.

Step 2. The Negatives. The second step was set to explore user pain points. It was completed in three stages planned to define and prioritize the potential problems of using e-ID. In the first stage participants were invited to write down their concerns and issues associated with the proposed e-ID platform in relation to their use cases. These statements could reflect potential drawbacks in the platform design from a human-centred perspective. Next, the participants had to vote for the concerns they deemed most important using the voting dots. With three of those dots, they could vote for any idea placing one, two, or all three dots on one or more sticky note with a negative statement. Having voted on the ideas, the third stage was about a debate on the top-voted concerns and explaining priorities. Once the speakers finished sharing their meaningful comments the second step was complete. The participants were offered a five-minute break, which also gave facilitators time to prepare for the next exercise.

Step 3. "How might we...?". The third step was done in two rounds where at least five top-voted problems from the previous exercise (*The Negatives*) served as inputs. Framed as "*How might we...?*" the exercise was arranged as follows. To overcome the *Concerns* (from the second step), participants needed to devise *Solutions* and think of the *Benefits* they could get from them. The participants were randomly assigned to five parties for working in groups imitating the *World Café* method (Slocum-Bradley, 2003) in both physical and virtual settings. Online, the tables were adapted to breakout rooms with separate dashboards on a digital whiteboard. In the first round, participants worked on a *Concern* around a table (or in a breakout room) with their initial group ideating solutions for the problem. In the second round, some participants switched between the groups moving to another table (breakout room) to complement the solutions from the previous work and consider attainable benefits. Using the voting dots, they could also highlight most appealing or prominent solutions. In 30 minutes, the third step was done.

Step 4. Wrap-up. The final step of the co-creation workshop was essentially an informal discussion about the benefits and solutions that were devised so far. All participants could overview their statements selected by their priorities on a common dashboard to find resembling ideas and cluster them. These clusters could be labelled based on the perceptions and feelings evoked by the solution-in-mind. Once the participants finished sharing meaningful comments, the workshop was concluded with closing remarks about the results and a wrap-up of the session.

4.2 Data collection

The co-creation workshops were convened by facilitators from the partnering public administrations. Prior to sessions, the first author provided the partners with training in facilitation and working with the digital tools. The workshop template was disseminated for tailoring to the specifics of the respective study case, along with recommendations for the recruitment of volunteers and templates for participant consent forms compliant with General Data Protection Regulation (GDPR).

The public administrations organized the recruitment for inviting residents and service providers who were interested in the proposed e-ID platform. They selected participants based on their knowledge of the end-user population contacting local networks and communities via email and in municipal premises. Table 2 provides with the summary of the workshop demographics. In one instance, the case owners

were unwilling to involve target users (vulnerable citizens) due to challenges for their direct participation. This has been considered a limitation to our study as not entirely co-creative approach.

Due to ethical considerations, the invitees enrolled by giving their informed consent, along with demographic information and permission to collect the materials (recordings, pictures, minutes, etc.) produced from workshops. For data management, each public administration and the research group signed bilateral data processing agreements specifying data processors and controllers. Following the agreements, the workshop materials were collected and stored in data management facilities of the respective public administrations, on behalf of data controllers.

Workshop theme	Format	No. of attendees	Stakeholder groups	Gender ratio (female/male)	Age group
Document lockers in the selected Danish municipality	Virtual	11	Shelter workers and municipal public servants	6/5	35-54
Filing crime complaints online in Spain	On-site	17	Citizens, police officers, investigation agents	0/17	35-54
Citizen card in the selected Spanish municipality	On-site	15	Citizens, municipal officers, and public service providers	9/6	35-45
E-government public services in the Bulgarian municipality	On-site	15	Health care and education workers, (unemployed) citizens, bank officers, lawyers	12/3	35-45
Italian business register for entrepreneurs	Virtual	13	Entrepreneurs, IT specialists, national public authorities	2/11	45-55

Table 2. The workshops demographics.

The sessions lasted 90 minutes on average. In virtual format, participants were instructed in how to navigate the digital whiteboard before proceeding to the exercises. The sessions were conducted in native languages of the locations, and the partners prepared translations and summaries with access to the pre-processed data.

4.3 Qualitative analysis and coding

For coding and qualitative analysis of the user statements (textual and verbal), we employed integrated elements of top-down (*a-priori*) and bottom-up (open coding) approaches. The former provided with high-level categories derived from the core functionalities of the proposed e-ID platform (i.e., "onboarding", "authentication", and "management of verifiable credentials"), along with the software quality characteristics (e.g., system's usability, security and their subcharacteristics) from ISO 25010 (2011). The latter allowed for identifying patterns and relations between the statements to compare against other for similarities and differences (Strauss and Corbin, 1998).

In a cross-case comparison, the statements were first clustered by the exercise stages: the positives, the negatives, and the proposed solutions. We then reframed those clusters to reflect the nature of statements and further transform them into requirements. For classification, we assigned numeric codes indicating study case origin, nature of the requirement (i.e., 01 – positive expectations, 02 –user pain points, 03 – user needs), and a serial number aggregating similar concepts. As the statements were prioritized by the participants, we selected the most prominent ideas and challenges, and mapped them against the corresponding categories from the referenced software quality model. This resulted in attributing the user statements to the quality characteristics identifying them as the kinds of requirements for the proposed e-ID management platform.

5 Findings

The workshops emerged as the first instance of dialogues between the public administrations and their local stakeholders. Citizens and public servants reflected on shared contextual environments for using e-ID from their own perspectives. We observed that the demo video of the onboarding process proved to be effective in its role as a boundary object (Leigh Star, 2010) adapting to each individual study case. Drawing on a prototype helped to inspire participants in the sense that they could form broader topical dimensions for consultations and debate. The examples of these dimensions included:

- the undergoing digital transformation of public services (e.g., *"To be completely honest, we think it is an enormously interesting e-ID solution, but as with everything else in the digital society there are always some barriers"*),
- usability and accessibility of online instruments (e.g., *"I think the [vulnerable] citizens that won't be able to make a use of a smartphone […] we will have exempted from the use of digital self-services"*, *"[This e-ID] can turn into an excellent alternative to the digital signature"*),
- contexts of verifiable identification (e.g., *"Businessmen usually delegate the access [to company's information] to secretary or other. Is this an issue?"*, *"[AI algorithms] should not be used for [validating complaints on] serious crimes"*).

With the set attitude, the participants proceeded with the exercises to discuss their ideas of the e-ID platform and its desired properties. In the following subsections, we describe our findings in relation to the research question as to what kind of requirements for the e-ID management platform the participants elicited in the workshops.

5.1 Onboarding e-ID platform

The first implications from the e-ID platform were resource and time **efficiency** which would facilitate identification processes for the participants (e.g., *"Less passwords to bear in mind"*, *"Motivating and very useful for electronic administration"*). This also implied the redundancy of visiting municipal premises physically through the enhanced online experiences (e.g., *"I will not move to the police station again"*, *"It will facilitate the digital interaction between citizens and municipality"*).

Thereafter, the participants recognized barriers in the e-ID platform's **accessibility** for the elderly people and vulnerable citizens (e.g., *"They [vulnerable citizens] usually don't even know how to use a smartphone. So, they will need a lot of help"*, *"Difficult to explain to older people"*). They made comparable remarks to prerequisites for educating and assisting the end-users with e-ID onboarding (e.g., *"Citizens are more confident and feel safer, when a representative of the municipality assists the process of registration"*, *"[We need] informative talks on the use of the [e-ID] tool in elderly people's centres"*).

In addition to the external **usability** support, the participants were advocating the means of spoken and video descriptions in system's user interface for accompanying the onboarding process (e.g., *"Support with a sound/voice file, not only written instructions"*, *"Explanation videos available [for using e-ID]"*).

These comments further led to forming ideas around **interoperability** of the platform with external interfaces, steering the discussions to technical angle (e.g., *"[It is] working just on one device"*, *"I just wondered whether it would be easier if they [vulnerable citizens] could be […] identified by an integrated camera in the document box"*, *"Possibility for family members to file the [crime] complaint on their [elderly people] behalf"*).

5.2 AI-based authentication

Contrary to the aforementioned efficiency benefits, the most recurring issues were linked to **reliability** of the AI-based functionality in e-ID platform. In all five workshops participants expressed their doubts about the facial recognition performing in various conditions (e.g., *"Drug affected citizens cannot always handle to take a selfie"*, *"Can the document box be accessed if [citizen's face changed] due to violence or makeup?"*, *"Problem with selfie – inadequate lightening, or using a facemask"*). They

further questioned **security** of the facial recognition as the only authentication method (e.g., *"[Can] using only photos make identity theft easier?"*, *"What if two people look very similar?"*).

It was noteworthy, that the biometric authentication was not found intrusive per se. In fact, in many cases the participants were rather enthusiastic about it, given the perceived **usability**, and suggested using even fingerprint or voice recognition (e.g., *"It could be possible to access services also through voice recognition via call centre"*). However, "conventional" login techniques for multi-factor authentication were considered as well (e.g., *"Provide the system with a double authentication"*, *"OTP (one-time password) code to be sent to the phone, to make the process safer"*).

In two workshops, primarily the public servants were sceptic about the **non-repudiation** of citizen identities' verification relying solely on AI algorithms. They therefore backed retaining manual control over verification process by the authorities, at least on the onboarding stage (e.g., *"It is good it is validated by a human, given the possibility that [AI] deviates from its purpose"*).

5.3 Management of verifiable credentials

We noticed that the SSI-principle (i.e., users control their own data) received rather faulty image as **security** and **data protection** were much debated. Few participants recognized DLT-enabled features as general benefits (e.g., *"A 'democratic' solution citizens own by themselves. Data not controlled by authorities"*, *"Confidence in that personal data are not stored on multiple servers"*).

However, in all the workshops the participants expressed concerns about **confidentiality** and **integrity** of their privacy and personal data treatment linked to just one device (e.g., *"It's a risk that people know where you store your personal information and therefore [user] can be threatened to open the document box"*, *"Leakage of personal data [due to] lost/stolen smart device"*, *"The state monitors"*).

Hence, the participants required **accountability** for data processing and transparency for verifiable credentials management (e.g., *"Where are my data stored?"*, *"How do photos get processed and stored?"*). They also devised sophisticated **security** mechanisms to ensure control over their electronic identities (e.g., *"[…] photos should be dumped right after the usage of them (no photo storage)"*, *"The tools should be able to detect fakes"*, *"The app could ask the user to correct biometric data"*, *"Retrain [the* AI algorithms of] the system on demand or periodically").

Lastly, from these dialogues the public servants realized some of the potential changes and risks in relation to their administrative workflows (e.g., *"The police officer doesn't have the chance to ask about the complaint. Close contact with citizens will lose"*, *"We previously had issues that [vulnerable] citizens used [document boxes] to store drugs. But now, with [e-ID solution] we will know which [drawer] belongs to respective users"*). These observations motivated the case owners to reflect on the public services selected for the project and formulate specific constraints for technologists to direct the e-ID platform design suited to their contexts.

5.4 Summary

In five co-creation workshops, the participants of different backgrounds shared their implications of a common e-ID management platform for online public services. They envisioned their interactions with the AI- and DLT-enabled software solution through the structured dialogic activities. The positive expectations from the e-ID platform were primarily associated with the increased usability, namely the efficiency and convenience of online public services access. However, accessibility, reliability, and security perceptions were confronted with technological propositions of the digital platform. The participants expressed the needs for comprehensive support for the various users of the e-ID management platform, as well as the reassurance of security and control over their personal data. We summarize the results of the workshops in Table 3 below and discuss the findings in the following section.

User statements	Onboarding	Authentication	Management of VCs
Positive expectations	Efficiency (resource utilization): *redundancy, self-service solution*	Usability (efficiency, resource utilization): *speed & efficiency, password-less*	Efficiency (resource utilization): *data redundancy* Security (integrity): *data control distribution*
User pain points	Usability (accessibility, appropriateness recognizability): *non-expert users, smartphone dependency*	Reliability: *facial recognition accuracy* Security (confidentiality): *identity theft, forgery*	Usability (appropriateness recognizability): *DLT misconception* Security (confidentiality, integrity): *data protection, tracking, hacking*
User needs	Usability (learnability): *assistance, user interface* Compatibility (interoperability): *Multiple interface support, data transfer between devices*	Usability (operability): *backup biometrics* Security (non-repudiation): *multi-factor authentication*	Security (accountability, confidentiality, integrity): *data transparency, data control*

Table 3. User statements, concepts, and corresponding quality attributes.

6 Discussion

The aim of our study was to identify what kind of requirements users have for the e-ID management platform in public sector. We approached this inquiry with the co-creation methodology to involve diverse stakeholder groups from five different case sites in dialogic, sense-making workshop activities. Participants' ideation was particularly evolving around accessibility, usability, and security aspects of e-ID for online public services. The main implication of our findings is that the types of requirements elicited in the workshop sessions were embedded into socio-technical arrangements of distinct contextual environments. Reflecting on how we addressed the research question, we drew several conclusions based on our observations and the follow-up conversations with the project partnering organizations.

6.1 Implications for research

The participants' remarks about AI-based authentication left us to conclude that the application of this technology for electronic identification may evoke different narratives for various stakeholders (Sartori and Theodorou, 2022). For example, citizens perceived biometrics merely as a login layer or "fast" and "convenient" authentication tool to "get their job done". In contrast, despite the perceived efficiency benefits to their workflows, the public servants realized organizational risks for their decision-making processes. This observation finds reflections in contemporary policy initiatives and academic literature calling for regulating the use of AI by making it explainable, transparent, and trustworthy (Thiebes, Lins and Sunyaev, 2021; European Commission, 2023).

While these properties can be achieved by deploying AI in systems that use DLT, the trust-ensuring merits of the latter were not reciprocated by users in our study. We may speculate that this fallacy was evoked by the conceptual complexity of DLT technology for e-ID platforms which was also observed in empirical studies on decentralized identity management (Ostern and Cabinakova, 2019; Korir, Parkin and Dunphy, 2022). From the technical point of view, the privacy-preserving features of the SSI-model can help users evade the dichotomy between abiding the security principles and getting their job done (Garfinkel and Lipford, 2014). However, it is not the identity management itself that is the end-goal for the most users, but the services they request to solve the tasks without risking their trust or usability experiences (Dhamija and Dusseault, 2008).

Our findings suggest possible conflict of usability, security, and accessibility characteristics not only for e-ID platforms design, but also for their understanding between technical and social dimensions. The propositions of the SSI-principle such as trusted identification and user empowerment through personal data control can hardly be conveyed as the value drivers to users who are not ready for new technologies (Dunphy and Petitcolas, 2018). That is, just the design of e-ID management platform is unlikely to evoke the sense of responsibility for taking control over the digital assets, and hence, the user participation in those platforms (Bazarhanova and Smolander, 2020). Even though technology success is widely defined by its acceptance or adoption, the technology can be adopted without being fully accepted by users or, conversely, be scarcely adopted despite meeting its acceptance criteria.

Based on the co-creation experience, we recommend looking into *why* and *how* users interact with technological artefacts, and not being exclusively focused on *what* these artefacts can offer. Further research on the differences in understanding user-centred e-ID management across contexts and dimensions can support the design and development of truly user-centred software solutions.

6.2 Implications for practice

Although the present study is not an example of genuine co-creation approach, our implications can resonate for practice too. The co-creation workshops were not intended specifically for looking into users' familiarity with e-ID management and underlying technologies of the digital platform. Instead, the participants were encouraged to take the role of experts and bring their perspectives on how the SSI-based solution for e-ID could direct citizens' conventions to accessing public services. We find the results of our approach appealing for adapting this methodology to systems development in public sector.

Citizens are part of various complex social and organizational structures, and the awareness of the technologies, skills, and abilities to benefit from them are unevenly scattered among the prospective users. This may be especially pertaining to the vulnerable populations who are in risk of becoming "alienated by the technology" (Dunphy and Petitcolas, 2018). Just as identity management is not usable if it is not secure, it is not secure if it is not accessible. The e-ID platforms' inclusivity can be achieved by combining digital security with human security approaches (Coles-Kemp, Robinson and Heath, 2022).

The actual empowerment of the users may come not from the technologies, but from the approach to their design. Co-creation can foster the uptake and communication of collaborative, user-centred design practices among all the stakeholders, and result in accessible, usable and secure solutions (Jarke, 2021).

The platform owners can support achieving the well-functioning e-ID management by reaching out to their users through proactive dialogues and practices, engaging them in design processes. Increasing transparency, simplifying language, and translating complex technological mechanisms can help strengthen reputation of the base digital technologies in public sector.

6.3 Study limitations

This study has limitations primarily discerned from its approach. We are aware that the recruitment and logistical organization are the main factors that define successes and failures of research involving human subjects. In co-creation, diversity and involvement of stakeholders are the key elements. For geographical reasons, the researchers were limited in the workshops' conduct and recruitment processes.

For example, in the Danish case the recruitment of volunteers was entailed with challenges for immediate online participation of people from the target group. Therefore, the case owners contacted local communities to form a pool of the workshop attendees comprising the service providers, shelter employees, and municipal public servants who work with homeless people through various initiatives.

The workshops were conducted in local languages of the respective case sites. Therefore, it was recognized that the data collected from the workshops is the subject to several levels of interpretation. First, it was the user statements produced with the help of facilitators from the public administrations. And second, it was translated from the local language into English with automated tools, which could result in different stylistic representation of the initial statements.

Finally, given the contextual differences of the study cases, the workshop template had to be designed more as the general exploratory activity for capturing the requirements. Some participants were taking a dual role of citizens and public authorities. This approach could limit possible methods for data collection and analysis in individual cases, for example through the dialectical process.

7 Conclusion

The combination of AI and DLT technologies brings new opportunities and challenges for the adoption of e-ID management platforms based on the SSI-model. The goal of our study was to identify what kind of requirements users have for e-ID management platform in public sector. We approached this question within the context of large research initiative concerning the e-ID platform development for different European case sites. From the five workshops designed by co-creation methodology, we found that accessibility, usability, and security were the most required properties by the prospective users. Based on our observations, we conclude that the discussion around the e-ID management platforms' design needs to shift from the technical perspective to understanding their social and socio-technical arrangements. Recognizing the limitations of our approach for this study, we aim to continue exploring the user perspectives on e-ID management in public sector in future research iterations.

Acknowledgements

This study was undertaken as part of the project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101004459.

We thank the anonymous reviewers whose comments improved the manuscript considerably.

References

Alexopoulos, C. et al. (2019) 'How Machine Learning is Changing e-Government', in Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance. ICEGOV2019: 12th International Conference on Theory and Practice of Electronic Governance, Melbourne VIC Australia: ACM, pp. 354–363. Available at: https://doi.org/10.1145/3326365.3326412.

Allen, C. (2016) The Path to Self-Sovereign Identity. Available at: https://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (Accessed: 19 January 2023).

Bazarhanova, A. (2020) Managing change in a dominant infrastructure for digital identification. Doctoral Thesis. Association for Information Systems.

Bazarhanova, A. and Smolander, K. (2020) 'The Review of Non-Technical Assumptions in Digital Identity Architectures', in Annual Hawaii International Conference on System Sciences, p. 10.

Berente, N. et al. (2021) 'Managing artificial intelligence.', MIS quarterly, 45(3).

van Bokkem, D. et al. (2019) 'Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology'. arXiv. Available at: http://arxiv.org/abs/1904.12816 (Accessed: 9 June 2022).

Coles-Kemp, L., Robinson, N. and Heath, C.P.R. (2022) 'Protecting The Vulnerable: Dimensions of Assisted Digital Access', Proceedings of the ACM on Human-Computer Interaction, 6(CSCW2), p. 534:1-534:26. Available at: https://doi.org/10.1145/3555647.

Čučko, Š. and Turkanović, M. (2021) 'Decentralized and Self-Sovereign Identity: Systematic Mapping Study', IEEE Access, 9, pp. 139009–139027. Available at: https://doi.org/10.1109/ACCESS.2021.3117588.

Dhamija, R. and Dusseault, L. (2008) 'The Seven Flaws of Identity Management: Usability and Security Challenges', IEEE Security & Privacy, 6(2), pp. 24–29. Available at: https://doi.org/10.1109/MSP.2008.49.

van Dijck, J. and Jacobs, B. (2020) 'Electronic identity services as sociotechnical and political-economic constructs', New Media & Society, 22(5), pp. 896–914. Available at: https://doi.org/10.1177/1461444819872537.

Drobotowicz, K., Kauppinen, M. and Kujala, S. (2021) 'Trustworthy AI Services in the Public Sector: What Are Citizens Saying About It?', in F. Dalpiaz and P. Spoletini (eds) Requirements Engineering: Foundation for Software Quality. Cham: Springer International Publishing (Lecture Notes in Computer Science), pp. 99–115. Available at: https://doi.org/10.1007/978-3-030-73128-1_7.

Dunphy, P., Garratt, L. and Petitcolas, F. (2018) 'Decentralizing Digital Identity: Open Challenges for Distributed Ledgers', in 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 75–78. Available at: https://doi.org/10.1109/EuroSPW.2018.00016.

Dunphy, P. and Petitcolas, F.A.P. (2018) 'A First Look at Identity Management Schemes on the Blockchain', IEEE Security & Privacy, 16(4), pp. 20–29. Available at: https://doi.org/10.1109/MSP.2018.3111247.

European Commission (2021) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281 (Accessed: 12 May 2023).

European Commission (2023) Regulatory framework proposal on artificial intelligence | Shaping Europe's digital future. Available at: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (Accessed: 9 March 2023).

Floridi, L. (2020) 'Artificial Intelligence as a Public Service: Learning from Amsterdam and Helsinki', Philosophy & Technology, 33(4), pp. 541–546. Available at: https://doi.org/10.1007/s13347-020-00434-3.

Fridgen, G. et al. (2018) 'Challenges and Opportunities of Blockchain-based Platformization of Digital Identities in the Public Sector'. Available at: https://orbilu.uni.lu/handle/10993/44519 (Accessed: 18 February 2023).

Garfinkel, S. and Lipford, H.R. (2014) Usable security: history, themes, and challenges. (Synthesis lectures on information security, privacy, and trust, 11).

Giannopoulou, A. and Wang, F. (2021) 'Self-sovereign identity', Internet Policy Review, 10(2). Available at: https://policyreview.info/glossary/self-sovereign-identity (Accessed: 11 May 2023).

Gulliksen, J. et al. (2003) 'Key principles for user-centred systems design', Behaviour & Information Technology, 22(6), pp. 397–409. Available at: https://doi.org/10.1080/01449290310001624329.

Holgersson, J. and Karlsson, F. (2014) 'Public e-service development: Understanding citizens' conditions for participation', Government Information Quarterly, 31(3), pp. 396–410. Available at: https://doi.org/10.1016/j.giq.2014.02.006.

Holmström, J. and Hällgren, M. (2021) 'AI management beyond the hype: exploring the co-constitution of AI and organizational context', AI & SOCIETY [Preprint]. Available at: https://doi.org/10.1007/s00146-021-01249-2.

Iivari, J. and Iivari, N. (2011) 'Varieties of user-centredness: an analysis of four systems development methods', Information Systems Journal, 21(2), pp. 125–153. Available at: https://doi.org/10.1111/j.1365-2575.2010.00351.x.

International Organization for Standardization (2011) ISO/IEC 25010:2011(en), Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models, ISO. Available at: https://www.iso.org/cms/render/live/en/sites/iso-org/contents/data/standard/03/57/35733.html (Accessed: 23 October 2022).

Jarke, J. (2021) Co-creating Digital Public Services for an Ageing Society: Evidence for User-centric Design. Cham: Springer International Publishing (Public Administration and Information Technology). Available at: https://doi.org/10.1007/978-3-030-52873-7.

Jones, P. (2018) 'Contexts of Co-creation: Designing with System Stakeholders', in P. Jones and K. Kijima (eds) Systemic Design. Tokyo: Springer Japan (Translational Systems Sciences), pp. 3–52. Available at: https://doi.org/10.1007/978-4-431-55639-8_1.

Korir, M., Parkin, S. and Dunphy, P. (2022) 'An Empirical Study of a Decentralized Identity Wallet: Usability, Security, and Perspectives on User Control', in Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022).

Kujala, S. (2003) 'User involvement: A review of the benefits and challenges', Behaviour & Information Technology, (1), pp. 1–16. Available at: https://doi.org/10.1080/01449290301782.

Kujala, S. (2008) 'Effective user involvement in product development by improving the analysis of user needs', Behaviour & Information Technology, 27(6), pp. 457–473. Available at: https://doi.org/10.1080/01449290601111051.

Laatikainen, G. et al. (2021) 'Towards a Trustful Digital World: Exploring Self-Sovereign Identity Ecosystems', in Pacific Asia Conference on Information Systems. Association for Information Systems.

Lee, J.-J. et al. (2018) 'Design Choices Framework for Co-creation Projects', International Journal of Design, 12(2), p. 17.

Leigh Star, S. (2010) 'This is Not a Boundary Object: Reflections on the Origin of a Concept', Science, Technology, & Human Values, 35(5), pp. 601–617. Available at: https://doi.org/10.1177/0162243910377624.

Lindman, J., Tuunainen, V.K. and Rossi, M. (2017) 'Opportunities and Risks of Blockchain Technologies: A Research Agenda', in. Hawaii International Conference on System Sciences. Available at: https://doi.org/10.24251/HICSS.2017.185.

Liu, Y. et al. (2020) 'Blockchain-based identity management systems: A review', Journal of Network and Computer Applications, 166, p. 102731. Available at: https://doi.org/10.1016/j.jnca.2020.102731.

Lockey, S. et al. (2021) 'A Review of Trust in Artificial Intelligence: Challenges, Vulnerabilities and Future Directions', in. Hawaii International Conference on System Sciences. Available at: https://doi.org/10.24251/HICSS.2021.664.

Melin, U., Axelsson, K. and Söderström, F. (2016) 'Managing the development of e-ID in a public e-service context: Challenges and path dependencies from a life-cycle perspective', Transforming Government: People, Process and Policy, 10(1), pp. 72–98. Available at: https://doi.org/10.1108/TG-11-2013-0046.

OECD (2020) The OECD digital government policy framework: Six dimensions of a digital government. OECD Public Governance Policy Papers 02. Available at: https://doi.org/10.1787/f64fed2a-en.

Ostern, N. and Cabinakova, J. (2019) 'Pre-Prototype Testing: Empirical Insights on the Expected Usefulness of Decentralized Identity Management Systems'.

Runeson, P. and Höst, M. (2009) 'Guidelines for conducting and reporting case study research in software engineering', Empirical Software Engineering, 14(2), pp. 131–164. Available at: https://doi.org/10.1007/s10664-008-9102-8.

Sanders, E. and Stappers, P. (2012) Convivial toolbox: Generative research for the front end of design. Amsterdam: Bis.

Sanders, E.B.-N. and Stappers, P.J. (2008) 'Co-creation and the new landscapes of design', CoDesign, 4(1), pp. 5–18. Available at: https://doi.org/10.1080/15710880701875068.

Sanders, L. (2008) 'An evolving map of design practice and design research', Human Factors, p. 7.

Sartori, L. and Theodorou, A. (2022) 'A sociotechnical perspective for the future of AI: narratives, inequalities, and human control', Ethics and Information Technology, 24(1), p. 4. Available at: https://doi.org/10.1007/s10676-022-09624-3.

Seltsikas, P. and O'Keefe, R.M. (2010) 'Expectations and outcomes in electronic identity management: the role of trust and public value', European Journal of Information Systems, 19(1), pp. 93–103. Available at: https://doi.org/10.1057/ejis.2009.51.

Slocum-Bradley, N. (2003) 'Participatory Methods Toolkit: A Practitioner's Manual'.

Söderström, F. (2016) Introducing public sector eIDs: The power of actors' translations and institutional barriers. Ph.D. Linköping University. Available at: https://doi.org/10.3384/diss.diva-132737.

Strauss, A. and Corbin, J.M. (1998) 'Basics of Qualitative Research: Techniques and procedures for developing grounded theory (Fourth)'.

Thiebes, S., Lins, S. and Sunyaev, A. (2021) 'Trustworthy artificial intelligence', Electronic Markets, 31(2), pp. 447–464. Available at: https://doi.org/10.1007/s12525-020-00441-4.

Trischler, J., Dietrich, T. and Rundle-Thiele, S. (2019) 'Co-design: from expert- to user-driven ideas in public service design', Public Management Review, 21(11), pp. 1595–1619. Available at: https://doi.org/10.1080/14719037.2019.1619810.

Tuunanen, T. et al. (2019) 'From digitalization to cybernization: Delivering value with cybernized services', Scandinavian Journal of Information Systems, 31(2), p. 3.

Tuunanen, T., Myers, M.D. and Cassab, H. (2010) 'A Conceptual Framework for Consumer Information Systems Development', Pacific Asia Journal of the Association for Information Systems, pp. 47–66. Available at: https://doi.org/10.17705/1pais.02104.

Vergne, J. (2020) 'Decentralized vs. Distributed Organization: Blockchain, Machine Learning and the Future of the Digital Platform', Organization Theory, 1(4), p. 263178772097705. Available at: https://doi.org/10.1177/2631787720977052.

Whitley, E.A., Gal, U. and Kjaergaard, A. (2014) 'Who do you think you are? A review of the complex interplay between information systems, identification and identity', European Journal of Information Systems, 23(1), pp. 17–35. Available at: https://doi.org/10.1057/ejis.2013.34.

Whitten, A. and Tygar, J.D. (1999) 'Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.', in USENIX security symposium, pp. 169–184.