



A Qualitative Study of Adoption Barriers and Challenges for Passwordless Authentication in German Public Administrations

Jan-Ulrich Holtgrave

CISPA Helmholtz Center for Information Security
Hannover, Germany
jan-ulrich.holtgrave@cispa.de

Karola Marky

Ruhr University Bochum
Bochum, Germany
karola.marky@rub.de

Sabrina Klivan

CISPA Helmholtz Center for Information Security
Hannover, Germany
amft@sec.uni-hannover.de

Sascha Fahl

CISPA Helmholtz Center for Information Security
Hannover, Germany
sascha.fahl@cispa.de

Abstract

Public administrations provide critical services and manage sensitive data for a country's citizens. Recent phishing campaigns targeting public sector employees highlight their attractiveness as targets. Deploying state-of-the-art authentication technologies, such as FIDO2, can improve overall security. We conducted a mixed-methods study in Germany to understand better the practices and challenges of deploying passwordless authentication in the public sector. First, we conducted an online survey (N=108) among German public sector employees to gain insights into their experiences and challenges. Next, we partnered with an e-government vendor and performed an in-situ experiment. We let 11 employees from the public sector experience FIDO2 under real-world conditions. Our results show that only a minority of our participants were aware of current passwordless authentication procedures. In our experiment, FIDO2-based methods left an overall positive impression. Hierarchical and heterogeneous public sector structures and the need for more technical expertise and equipment were barriers to adoption.

CCS Concepts

• **Security and privacy** → **Usability in security and privacy**; Authentication.

Keywords

Authentication, Public Administration, E-Government

ACM Reference Format:

Jan-Ulrich Holtgrave, Sabrina Klivan, Karola Marky, and Sascha Fahl. 2025. A Qualitative Study of Adoption Barriers and Challenges for Passwordless Authentication in German Public Administrations. In *CHI Conference on Human Factors in Computing Systems (CHI '25)*, April 26–May 01, 2025, Yokohama, Japan. ACM, New York, NY, USA, 16 pages. <https://doi.org/10.1145/3706598.3713252>

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

CHI '25, Yokohama, Japan

© 2025 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 979-8-4007-1394-1/25/04
<https://doi.org/10.1145/3706598.3713252>

1 Introduction

Public administrations, such as registration offices, tax authorities, or social services, are critical providers of many services that process and store large amounts of sensitive citizen data. Past and current incidents illustrate that this makes public institutions an attractive target for cybercriminals [25, 26, 42, 44, 54, 76] and stress the importance of the successful deployment of security mechanisms. However, this domain received little research in the security literature, which is also shown by the most recent US National Science Foundation call that endorses security research in public administrations, as further insights are needed [45].

Public authorities, ministries, and other public institutions have very diverse working environments from private companies and start-ups. For example, public administrations often deploy specialized E-Government software from only a few vendors and are therefore under less pressure for innovation [12, 53]. Further, public administrations often seem to lack intrinsic motivation for change and updated processes because information technology procurement must pass complex and time-consuming processes [8, 49].

This special environment also poses major challenges for IT security integration and application. Szczepaniuk et al. [70] paint a worrying picture of the public IT in Poland, identifying human factors as one inherent security problem for this domain. Evans et al. [18] found that the share of security incidents based on human error was 51% in private organizations and even 91.5% in public sector organizations in the UK. This discrepancy reveals the special responsibility of employees in public sector organizations and the relevance of human-centered security research for this domain.

Despite these challenges and risks, many countries consider digitizing their infrastructures and services an essential success factor. Countries such as Germany, the UK, Canada, Romania, and the US announced massive investments in their digital sectors [14, 21, 28, 58, 63]. In sum: Improving IT security in public administrations is particularly critical and challenging. Further human factors need special consideration.

Passwordless authentication mechanisms aim to improve authentication security by replacing passwords [6, 20, 71] or introducing additional authentication factors [1, 43, 57]. FIDO2, in particular, is a passwordless authentication mechanism published by the FIDO Alliance [2] to improve security by better protecting against phishing attacks and password leaks [3, 41]. Time-Based One-Time

Passwords (TOTP) provides one-time passwords via separate devices or apps [50]. Previous studies uncovered multiple adoption and acceptance challenges of passwordless authentication mechanisms for end-users [19, 20, 41, 61, 62] and in organizations [30]. It is an open question how the unique environment of public administration [11, 22, 69] impacts the deployment of passwordless authentication.

In our exploratory study, we examine what hurdles and possibilities exist for security technologies and whether this domain has other issues with passwordless methods. We specifically focus on Germany to make the study more comparable with previous studies using mostly German populations [19, 20, 38, 39] but also because we had the opportunity to cooperate with an e-government vendor that is primarily active in Germany.

Our research questions are as follows:

RQ1 What passwordless methods are currently used by German government employees, and how are they perceived? We identify methods that are already used by public administrations and learn about employees' perceptions.

RQ2 What domain-specific barriers and benefits exist when introducing passwordless authentication methods, like FIDO2, for employees of public administrations in Germany? As the public sector faces unique challenges in IT projects, we investigate obstacles and possible benefits when implementing security measures such as secure authentication.

RQ3 What can be improved for public administrations in Germany to achieve a higher adoption? Based on our findings, we recommend using such authentication technologies in public administration and how barriers can be reduced.

To answer our research questions, we performed an exploratory mixed methods study: (1) an online survey (N=108) and (2) an in-the-wild user experiment with a follow-up interview (N=11). For the survey, we asked 108 employees from the German public sector about their previous experiences with passwordless authentication (RQ1). In the second study, we added FIDO2-based and TOTP authentication to the Integreat content management system (CMS) which is widely used within the public sector in Germany¹, which eleven participants used for at least two weeks. We tracked their authentication usage, and in a follow-up interview, we asked our participants about their experiences with the login procedure, their personal preference of the most common passwordless authentication methods, and their attitudes towards introducing such methods in their work context (RQ2, RQ3).

Our findings illustrate that public authority employees can use FIDO2-based authentication, but internal regulations may prevent them from doing so. It is primarily up to the public decision-makers to reform these rules, e.g., to exempt FIDO2 hardware keys from the ban of external USB storage devices or to make TOTP-powered authenticator apps mandatory in managed government app stores. That way, decisions on security measures can also be made decentrally at the departmental level, and an overall greater demand

can also provide an impetus for more security in e-government software.

Research Contribution. With our paper, we make the following contributions:

- **Investigating Authentication Methods in Public Sector Organizations:** We report the prevalence of authentication methods in our sample of German public administration employees — 35% of the participants of the survey reported to have used passwordless authentication at work; most participants used authenticator apps (TOTP).
- **Perception of Passwordless Authentication:** Our results suggest that most participants generally liked passwordless authentication, particularly FIDO2. Conversely, only some participants liked TOTP apps, as only a few employers provided service smartphones, and authorized TOTP apps were only available in a few cases.
- **Information Security at Public Administrations:** We show that a lack of technical expertise and complicated hierarchical decision-making processes within the public authorities mainly hinders adaptations within the domain.
- **Security Research with Public Administrations:** As this is one of the first security studies with government employees, we can provide hints for further research. For example, we experienced no established processes that allowed interested participants to participate in our studies, making recruitment particularly challenging.

2 Background

This section summarizes the investigated authentication methods and their security benefits. We further contextualized the security benefits with five common attack vectors against passwords. Details about the functionalities can be found in Appendix B.

2.1 Time-based One-Time-Passwords (TOTP)

TOTP is based on the procedure for generating one-time passwords (OTP) but adds a temporal component as an additional security mechanism (see RFC 6238 [50]). Hence, after creating an OTP, it is only valid for a defined time window. Modern procedures use a shared secret (e.g., via a QR code) between the authentication service and a client for the OTP generation. The shared secret is usually invisible to the user and randomly generated at a sufficient length to protect against brute-force attacks. Unique secrets are generated for each authentication service, so only one service is affected if a leak occurs. Secrets should never leave the device, and only temporary OTPs are exchanged to protect against Man-in-the-Middle (MitM) attacks. The retrieval of the OTP typically happens via a second device (e.g., smartphone, TAN generator) whose authentication should be protected against theft. Dmitrienko et al. [15] concluded in their analysis that TOTP procedures offer several security features, yet the smartphone as the underlying medium introduces most of the attack vectors.

2.2 Fast Identity Online 2 (FIDO2)

FIDO2 is developed and maintained by the FIDO Alliance and the World Wide Web Consortium (W3C) to provide a secure alternative to passwords [2]. Major industry partners, such as Microsoft and

¹Integreat-CMS is an open-source tool offered by the Tür und Tür Digitalfabrik gGmbH as a Software-as-a-Service solution for the public sector. Referred to as **IG-CMS** from here on.

Apple, and FOSS organizations, such as Mozilla, are part of the alliance and support the standard in their products. FIDO2 uses a public-key-based challenge-response procedure for authentication, so intercepted communication is mostly uncritical. Authentication between a client and a relying party (RP) always occurs on a domain basis, so FIDO2 is considered to be phishing-resistant. This means that a user cannot be tricked into authenticating on a malicious domain similar to a known service. Leaks of public keys are also not critical since these must be known for authentication between clients and services. Regarding theft, a distinction must be made between (roaming) hardware tokens and procedures using a built-in Trusted Platform Module (TPM). In the case of TPMs, the device on which the client is running is authenticated, and, as with TOTP, this should be secured by user authentication. With roaming tokens, authentication takes place via a device connected via USB. These USB tokens can be used on different devices and can, therefore, be stolen and put to use. However, devices can be secured via an additional factor, such as a PIN, and the device locks after five incorrect entries. If a second factor is set, the theft of a token is troublesome but doesn't affect the security. There have been some small security issues related to FIDO2-based authentication [36], but the overall security claims are still withheld.

2.3 Summary

Table 1 summarizes the security claims of the authentication methods versus common security vectors for authentication.

3 Related Work

In this section, we discuss previous related work in two key areas: user studies on passwordless authentication and human-factors research within the public sector.

3.1 FIDO2 Authentication

Since FIDO2 as a standard does not require a uniform implementation, a distinction must be made between a roaming setup and a setup with Trusted Platform Modules (TPM) when considering usability [3]. Some studies have examined the usability of physical roaming tokens for authentication. Lyastani et al. compared the usability of FIDO2 tokens with password-based authentication in a single-factor setup with 94 users [41]. They used YubiKeys, and the study results indicated that users are willing to use FIDO2 instead of password-based authentication. Farke et al., who conducted a lengthier qualitative study on the use of FIDO2 within smaller companies, reached a different conclusion. One part of the group described the use as very pleasant, but the other half saw some obstacles. Mentioned barriers are the fear of losing the physical token, and the more time-consuming procedure [20]. In addition, there appear to be several other issues regarding physical FIDO2 tokens. A study by Reynolds et al. pointed out the difficulty of the setup process of YubiKeys for FIDO2 authentication [62]. Users who did not have guidance in the setup process often failed to associate the key with their account correctly. However, most subjects had very positive experiences using the tokens in action. Other studies focused on the duration of login ceremonies. Reese et al. and Farke et al. show that hardware tokens initially seem to increase users'

login time but reduce it significantly over time. Ultimately, login times are comparable to other methods [20, 60].

Another variant of FIDO2 authentication is the use of TPMs, which are installed in the systems as hardware chips. Farke et al. studied Windows Hello among users in a smaller company [19]. The users liked the method and saw advantages over the previous password variant. However, the study did not demonstrate the usual preference for biometric security over using Personal Identification Numbers (PINs). However, the authors attributed this to a lack of hardware and the participants' spatial situation. For example, some devices did not have the technical equipment for biometric authentication or were stationary, so fingerprint sensors were not easily accessible.

3.2 TOTP Authentication

The usability research of TOTP generally seems to focus more on a comparative level with other authentication methods. For example, Reese et al. noted in their comparison of five authentication methods that TOTP is relatively understandable for users, but there are still some usability problems. For example, the QR code was not scanned with an authenticator app, and the codes' time limit led to failed authentication attempts. This method also has the longest setup time in the study and the worst Single Easy Question (SEQ) score [60]. Reese also noted the same problem with timeouts with TOTP. However, the participants in the study rated TOTP as the method with the highest usability after passwords [61]. In general, previous research on TOTP seems to show that the method is easy to understand and considered secure [35]. Still, authenticating takes a comparatively long time, and some failed authentication can occur due to handling.

3.3 Public Administrations

With a stronger focus on e-government services, there appears to be an increased interest in usability studies of government software. However, recent research is mainly focused on UI/UX aspects of public applications (government websites, online services, etc.) [5, 10, 23, 56, 75].

Little attention has been paid to the employees of public administrations and their perspective on software. A case study by Cajander et al. investigated the relevance of usability within the Swedish Student Financial Aid Authority IT systems. It was shown that from the perspective of HCI researchers, little importance is attributed to the software's usability, but efficiency, legal certainty, and economic aspects are the strongest factors. In addition, the study indicates that the users have little to no participation in the design and further development of the software. Rather, "*orderliness, objectivity, and control*" are the central success factors for the authority studied [12]. Another study by Følstad et al. on the role of HCI in the design of public software in Norway concludes that while project managers often assume that end-users are sufficiently involved in projects, other studies point to the lack of user involvement as the leading cause of failed e-government projects [24]. Szczepaniuk et al. [70] analyzed IT security within the Polish public sector and identified numerous problems. These include the "*lack of ISMS organization*", the "*lack of reviews, audits or controls*", the "*limited use of physical and technological protection measures*", and

Table 1: Security benefits against common attack vectors.

Method	Dictionary Attacks	Phishing	Protection against:		
			Leaks	Man-in-the-Middle	Theft
Passwords	○	○	○	●	●
TOTP	●	●	●	●	●
FIDO2 with Hardware Token					
Without Pin	●	●	●	●	○
With Pin	●	●	●	●	●
FIDO2 with TPM	●	●	●	●	●

Scale: Strong protection(●), Medium protection(●), No additional protection(○)

the “lack of [employee] training” as massive problems for security. In a UK-based study, Evans et al. [18] made a comparison of IT security incidents between public and private organizations and found that the proportion of incidents based on human error was 51% in private organizations and as high as 91.5% in public sector organizations.

4 Online Survey

In this exploratory survey, we investigate the use of and experiences with passwordless authentication in German public administrations. We survey deployed methods, their perception by public administration employees, and the general view on information security. Overall, 108 public administration employees from more than 50 different public administrations in Germany participated in the survey. We collected answers from October 2022 to February 2023.

4.1 Recruitment

We used snowball sampling for recruitment, using our professional network and official communication channels from IG-CMS. The condition for participation in the survey was current employment in a German public administration or employment at an organization that has taken on official functions on behalf of the German state. Table 2 summarizes recruitment actions and the approximate number of employees we reached.

Table 2: Recruitment channels and approximate number of people reached.

Method	Contacts
Social Media Posts	113
Blog Entry	22
Municipality partners	98
Newsletter	142
Online workshops	39
In-person recruitment	27
Professional contacts	44
Sum	485

4.2 Questionnaire

We used a Qualtrics² server to collect survey questionnaire responses. The survey comprised five sections, which are described below. We provide the German questions and an English translation in our replication package (Section A).

Introduction. Employees could only participate after signing a consent form (see replication package). We further described the study, provided contact information, and illustrated all the data we intended to collect in the survey. Participants had to be of legal age and able to speak and understand German.

Demographics. This part of the survey consisted of standard demographic questions about age, gender, federal state of residence, level of education, and type and area of employment.

Recruitment for Usability Experiment. In this optional part, we asked participants if they were active users of IG-CMS to assess their qualifications for the second study. For this purpose, we inquired about technical requirements, such as the availability of service smartphones or USB slots in their work devices. If they met our conditions, we invited them to the second study described in Section 5.

Self-Assessment of Cybersecurity Knowledge. In this section, we asked participants about their familiarity with various cybersecurity terms to identify cybersecurity technologies deployed in German public administrations. We used a modified self-assessment version for Web-Use Skills [31]. We focused on questions related to cybersecurity and broader authentication methods, including *Windows Hello* and passwordless authentication [20].

Use of Passwordless Authentication Methods. The last survey section focused on passwordless authentication methods participants had used in the past. The initial question graphically depicted and briefly explained biometric authentication, hardware tokens, TOTP, and public key infrastructure cards. Then, we asked participants to report their experiences with the described passwordless authentication technologies in their work and personal lives. We distinguished between technologies that participants were still using and those they had stopped using. We asked them for ideas to improve the usability of their technologies. We asked for the reasons for discontinuing the use of passwordless methods.

After completing this last section, we allowed participants to drop out of the study, delete their responses, or submit the survey.

²www.qualtrics.com

4.3 Results

We received 108 valid and complete survey responses, a **response-rate of 22.26%**. Table 3 illustrates the participants' demographics. The population is diverse regarding the work sector and age, but people under 30 were underrepresented. More than 70% of the participants had a university degree (Bachelor's or Master's).

The participants' IT services are provided mainly by their IT departments. They also work in medium-sized departments (department size: *mean* = 31.61, *median* = 15).

4.3.1 Self-Assessment of Cybersecurity Knowledge. Our survey presented participants with a 5-point Likert scale and asked them how familiar they were with several cybersecurity terms. The self-assessment of cybersecurity knowledge reveals a broad spectrum of answers. For example, participants were more often familiar with terms such as *Malware* or *Phishing*, while only a tiny group indicated that they had heard of *Windows Hello*, *Challenge-Response* or *Brute-Force*. About half of the participants were familiar with *Passwordless Authentication* and *One-Time Passwords (OTPs)*. Table 4 illustrates our findings.

4.3.2 Experiences with Passwordless Authentication. We further asked participants if they had ever used passwordless authentication methods in their work environments, and only 38 (35.19%) stated they had done so. As a follow-up, we asked open-ended questions about the methods and participants' experiences. We used a qualitative open coding approach together with affinity diagramming [13] to analyze the written responses (see Appendix A for the complete codebook). We excluded seven responses based on misconceptions regarding the definition of *passwordless authentication*. In these cases, participants reported "*Multi-*" and "*Two-Factor Authentication*" (MFA/2FA) as an independent authentication method or mentioned "*passwords*" as a passwordless authentication method. Figure 1 shows how frequently the authentication methods were mentioned. Authenticator apps, hardware tokens, biometric methods, and smart cards were primarily reported to be currently used or to have been used in the past.

We inquired participants about their previous experiences with each passwordless authentication method, the reasons for their introduction within its workplace, and the general IT setup in their

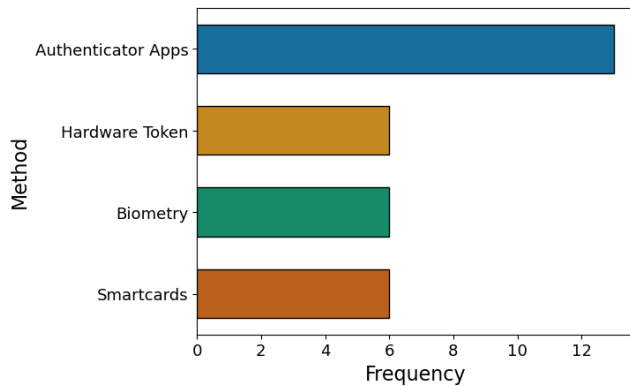


Figure 1: Frequency of mentioned methods.

Table 3: Demographics for all 108 valid participants from the online survey.

Demographics	Value	Percent
Gender:		
Male	56	51.9%
Female	52	48.1%
Non-Binary	0	0%
Age:		
20-29	9	8.3%
30-39	26	24.1%
40-49	23	21.3%
50-59	26	24.1%
>60	24	22.2%
Federal State:		
North Rhine-Westphalia	53	49.1%
Lower Saxony	20	18.5%
Hesse	12	11.1%
Bavaria	9	8.3%
Baden-Württemberg	5	4.6%
Mecklenburg-Western Pomerania	3	2.8%
Rhineland-Palatinate	2	1.9%
Schleswig-Holstein	2	1.9%
Brandenburg	1	0.9%
Saxony	1	0.9%
Level of Education:		
Diploma or equivalent	45	41.7%
Master's level or equivalent	23	21.3%
Bachelor's degree or equivalent	12	11.1%
Middle School Maturity	8	7.4%
High school diploma or equivalent	6	6.5%
Completed secondary education	7	6.5%
Doctoral degree or equivalent	3	2.8%
Magister level or equivalent	3	2.8%
Study without degree	1	0.9%
Employment Type:		
Full-time	69	63.9%
Part-time	30	27.8%
Fee-based	6	5.6%
Minor employment	1	0.9%
Prefer not to answer	2	1.9%
Field of Employment:		
Social Services	23	21.2%
Municipal Office	20	18.4%
Education	11	10.2%
Infrastructure and urban planning	10	9.3%
IT administration	8	7.4%
Semi-governmental administration	6	5.5%
Foreigners and Migration Services	4	3.7%
Consumer protection agency	4	3.7%
Economic development	3	2.8%
Employment services	2	1.9%
Other	14	13.1%
Prefer not to answer	3	2.8%

Table 4: Descriptive Analysis of Cybersecurity Knowledge Self-Assessment on a Scale of 1 (“No familiarity at all”) to 5 (“Very familiar”).

Familiarity Item	Median	Mean	SD
Malware	4	3.30	0.15
Phishing	4	3.67	0.13
Passwordless Authentication	3	3.03	0.14
OTP	3	2.81	0.15
Windows Hello	1	1.88	0.12
Challenge-Response	1	1.46	0.09
Brute-Force	1	1.78	0.13

German public authority. We illustrate the findings of the open coding analysis below.

Authenticator Apps. The participants reported that smartphone methods are or are most likely used by public authorities (13). In this category, we have combined methods such as Transaction Authentication Number (TAN) and authenticator apps (TOTP) on a smartphone. Three participants were disturbed by the fact that they needed a second authentication device: *“It’s inconvenient because I always have to have my cell phone to hand.”*

One participant further mentioned that passwordless authentication was more accessible and required less effort than passwords (1). Furthermore, one person mentioned that missing cell or Wi-Fi reception could complicate authentication.

Smart Cards. Some participants named smart cards as a method of use (6). Participants used them for accounting procedures or access management: *“[Public Key Infrastructure] cards for instructing payouts.”* However, some participants reported repetitive technical problems during authentication (2): *“Card recognition does not always work.”*

Hardware Tokens. Furthermore, external hardware tokens were standard (6), typically used to authenticate ballots: *“Authentication stick used in conducting elections and election data collection.”*

We summarized statements such as *“USB stick for authentication”, “Yubikeys”, or “External authenticators”* in this category.

Biometric Authentication. The last mentioned authentication method was biometric methods (6), in particular, fingerprint sensors (3): *“Service laptops with fingerprint scanners.”*

Incorrect recognition (1) was mentioned as a problem with the method. *“Recognition doesn’t always work, so I still often have to fall back on PINs.”*

Reasons for Deploying Passwordless Authentication. Most frequently, participants mentioned working in their *home office* (5) as a reason for deploying passwordless authentication in their work environment. They mentioned the need for a second factor when working from home: *“An additional authenticator in the office name plus password in the home office.”* This finding may be associated with expanding home office arrangements within the German public sector as a reaction to the global pandemic caused by the COVID-19 pandemic [52].

Broader Security Mindset. We identified further sentiments, allowing us broader insights into our participants’ perspectives on

cybersecurity. Some participants mentioned the regular change of passwords as an effective security measure (2). *“Secure password must be changed regularly.”* However, previous research found regular enforced password changes to be counter-productive [29].

Although participants described MFA procedures as being less usable, some described security benefits compared to passwords-only-based authentication ($N = 2$): *“Use of an MFA is inherently disruptive, and should be, namely to prevent unauthorized people from authenticating with stolen data or devices.”*

Key Findings – Online Survey. Our participants tended to be less tech-savvy but highly educated full-time employees from Western Germany. Only a minority stated that they have used passwordless authentication in their work environment. They were familiar with attacks such as malware or phishing, less so with protective measures like passwordless authentication. Most commonly, 12% mentioned exposure to TOTP-based methods.

5 In-the-wild User Experiment

This experiment explored the reception of passwordless authentication methods in German public administrations. To do so, public administration employees were exposed to these methods in a real-world scenario and incorporated them into their usual work processes. This experiment was conducted with our partner company, whose IG-CMS is actively used by several German public and semi-governmental social administrations. Within our experiment, IG-CMS implemented several passwordless authentication methods to secure access to our participants’ accounts. We conducted the experiment and interviews between December 2022 and April 2023. We describe the implemented methods and experiment conduction in the following.

5.1 Recruitment

We recruited participants through the initial online survey and distribution through the company’s network. In addition, we actively promoted our study during two live workshops with IG-CMS users, and the company’s partner managers were also asked to mention the experiment in their contacts with customers. In addition to recruiting employees from municipalities, we also recruited participants who worked in administrations from German initial reception centers for refugees. Semi-governmental organizations run these centers for the German federal states, and IG-CMS is used in some of them. To avoid distortion in the data, we ensured that only users of IG-CMS were recruited who also took on administrative government functions (e.g., recognition, registrations, or enrollment). Our recruitment measures and the approximate number of people reached in Table 5.

After participants expressed their willingness to participate in the experiment and fulfilled the participation requirements, we arranged a setup meeting by telephone or email, in which we also clarified questions and experiment details if necessary.

5.2 Implementation of Authentication Methods

For the qualitative user study, IG-CMS set up another login link for the users of the e-government software. In case FIDO2 was used, participants either utilized Windows Hello or required a hardware

Table 5: Experiment recruitment and approximately reached individuals.

Method	Contacts
Emails to municipality partners	98
Recruitment during online workshops	39
Recruitment during physical workshops	27
Direct recruitment calls	17
Total	181

token. In the latter case, we provided participants with a FIDO2-certified hardware token from Yubico³, which we allowed them to keep even after the end of our study. Furthermore, IG-CMS kept the alternative authentication methods active for participants who preferred it over their traditional password-based authentication. To authenticate, participants required a previously assigned PIN, and, in the case of the security keys, participants further needed to confirm the procedure physically.

In the case of TOTP, participants were required to enter the number from the connected Authenticator app.

5.3 Setup Meeting

As previous work has already studied the setup of passwordless authentication [60, 62], and as we were unable to meet most of our participants in person for a setup study in a suitable lab environment, we chose not to study the adoption process and instead include the method setup as part of our study onboarding [19, 20, 41]. Based on our experiences during this experiment, we further found that this helped our non-tech-savvy participants overcome initial challenges and participate in the two-week period to test passwordless authentication in their work environment. The setup meetings took place after confirming participation and fulfilling possible further conditions, such as legal agreements with the county. Before the setup meeting, participants were asked which of the following methods would be possible under their work circumstances:

- FIDO2 with Roaming Token (YubiKey)
- FIDO2 with TPM (Windows Hello)
- (Backup) TOTP with Authenticator App

Participants with FIDO2 hardware tokens had to receive the hardware tokens before the setup. Within the setup meeting, we set up the authentication methods that participants chose or could use. However, based on organizational constraints such as a lack of corporate phones or the deactivation of Windows Hello within managed software, most participants chose YubiKeys for our experiment. Setups happened either via videoconferencing or in person at the municipality. All procedures were set up as single authentication factors to focus attention on the authentication methods themselves and to keep the study comparable to those of Farke et al., Lystani et al., and Owens et al. [19, 20, 55]. A 2FA setup would have resulted in a different usability experience, as Farke et al. also argued in their study [20].

After the method was deployed, a two-week phase commenced, during which the participants were instructed to use this alternative

login. The design and duration of the experiment were designed based on previous work [60], and other research has shown that due to habituation effects, novel findings decrease after two weeks [34]. We, therefore, chose to limit our study length so as not to obstruct or affect our participant's work environment longer than necessary.

5.4 Collection of Metadata

For the entire experiment duration, IG-CMS collected additional log data about our participants' authentication procedures. These consist of the start of the login process (web request of the passwordless login link), additional logs related to the authentication via a passwordless method, and the redirect on successful authentication.

5.5 Semi-Structured Interviews

After participants had used their chosen authentication method for at least two weeks, we scheduled semi-structured exit interviews. In these interviews, we asked them about their experiences, perceptions, barriers, and possible improvements with their passwordless authentication methods. The exit interviews took an average of 20 minutes and were conducted in German. All but one of the interviews were conducted online via Webex or Jitsi. The single offline session was necessary because the IT security officer had to check the YubiKey setup on-site. The interviews were recorded using OBS⁴.

The interview guide can be divided into five distinct parts. Their respective objectives are explained below, and the complete interview guide can be found in the replication package (see Appendix A).

Consent. First and foremost, we reiterated the study's context and informed the interview participants about the study's process and purpose. We further asked for consent to record the exit interview. Additionally, any remaining questions were clarified. We started the interview after the participants had agreed to the recording.

Work Environment. In terms of content, participants were first asked additional questions about their background and work environment. Since the participants had already taken part in the previous online survey, the key demographic characteristics of the participants were already known (compare Section 4). Still, we asked participants to elaborate further to gain insight into their employment and working conditions. We asked, for example, about their daily contact with sensitive data and existing security considerations or guidelines.

Experiences with the Method. This section addresses topics that can be directly derived from the research questions. We asked participants to talk about how they liked their authentication method, whether they had problems during the experiment, and whether they had any suggestions for improvements. Furthermore, based on the survey answers, we asked them about their previous experiences with other passwordless methods and their usage at their workplace. This should also help to consider the more general use of such methods, not only the one with which the participants gained experience during the experiment. For the design of the individual questions, we used the studies by Farke et al. from 2020

³<https://www.yubico.com/de/product/security-key-nfc-by-yubico/>

⁴<https://obsproject.com/>

and 2022 as a starting point to achieve good comparability of the results [19, 20].

User Experience Questionnaire. Following the qualitative examination of the authentication methods, we took a more structured approach to evaluate the processes with the help of the User Experience Questionnaire Short (UEQ-S) [66]. The UEQ-S is a structured approach for evaluating digital and interactive products from a UI and UX perspective [40, 67]. We chose the shortened version for the interview because it provides good product classifications despite its brevity, and we would rather exhaust the participants during the interview [66].

Follow-up Questions. For the last part of the interview, we prepared some follow-up questions in case the respective topics had not already been addressed in the previous parts. To form these questions, we consulted previous findings from other studies by Farke et al., Reese et al., Owens et al., and Wuersching et al. to, e.g., address concerns like the loss of the FIDO2 hardware key or a possible improvement by removing the PIN entry [19, 20, 55, 60, 61, 77]. We also asked for their opinion on the potential use of the tested authentication method in their department. We then did the same for the other Windows Hello and TOTP methods, presenting their main features and benefits. After the follow-up phase of the study, we allowed participants to ask questions or discuss additional topics that had not been mentioned previously, and the study was concluded.

Debriefing. We included a debriefing phase after the interview for participants who had further questions about the interview or the entire study. In this phase, the participants could ask questions, or we could discuss possible assumptions about the erroneous authentication method. In some cases, we discussed the deactivation of the additional login link.

5.6 Data Processing & Analysis

Various data types were collected during the experiment, which are treated and evaluated differently. First, we generated login patterns from the collected metadata and calculated the time delta between the start of authentication and successful forwarding. For this purpose, we used the individual timestamps from the logs, and their delta was assigned to the participants. This was done to show possible habituation effects for the authentication times [20, 55].

To analyze our semi-structured interviews, we followed the six-step thematic analysis approach by Braun and Clarke [9, 13]. After getting familiar with all transcripts, one author proposed an initial codebook. This codebook, on the one hand, used codes from Farke et al. [19, 20] to allow a better comparison between the domains of public and private sector organizations. On the other hand, we added new codes based on our data connected to usability issues like *Fear of breaking the Hardware Token* or codes that refer to the perceived security of the authentication method like *Key more secure*. Hence, we applied semi-open coding.

After finalizing the codebook and discussing it with a second researcher, two coders independently coded all interviews. Afterward, we solved all conflicts through discussion and agreed on final code allocations. Following previous work, we omit the reporting of an inter-rater reliability score as our conflict solving approach leads to a hypothetical agreement of 100% [7, 46, 47]. The complete

analysis was done with the original German transcripts, and the codebooks were also created in German. For the publication, codes, themes and quotations were translated into English. We provide a list of all quotations used together with the original German in the Supplementary Material (see Appendix A) to verify our translations. After the eighth interview, no new topics emerged and we finished the experiment for the last three scheduled participants for additional empirical stability. Because of this, and given that we have recruited participants from seven different independent public institutions from all over Germany, we conclude that we reached thematic saturation as defined by Saunders et al. [65] for the interview analysis. Once, all interviews were coded, we used affinity diagramming to derive comprehensible themes based on codes that are related to each other, such as identified usability issues, the perceived security of FIDO2, and the public sector domain.

Finally, we also used the benchmarking class of Hinderks et al. [32] to evaluate the UEQ-S score.

5.7 Results

Overall, we conducted our in-the-wild experiment with eleven participants from seven different public authorities across Germany. The recruitment measures achieved a **response-rate of 6.08%** considering the approximate number of people reached. However, during our recruitment, we observed several obstacles for participants, such as requiring official forms before employees were allowed to participate or organizational issues, such as managed software, policies against USB slots, and shared computers, that led to several interested users ultimately declining our invitation. All participants completed the experiment and thus gained at least two weeks of experience with the respective authentication method. Table 6 illustrates the participants' demographics and authentication methods.

The table shows that the participants are evenly distributed in terms of gender and that several German states are represented. Most participants were between 30 and 49 years old. None of the participants used a TOTP setup, and only one used Windows Hello. This was not intended for the experiment. However, some major organizational hurdles arose in setting up these methods, which still provides insight into this domain's organizational barriers (see Section 8). The main issues hindering TOTP usage were the lack of service smartphones required and the fact that even if a service cell phone was available, IT was often managed centrally, and no authenticator apps were available or could be installed. Windows Hello was prevented for organizational reasons since authentication via Windows Hello was not possible according to the *Windows Group Policies* of the respective municipal IT or because of the age of the used devices.

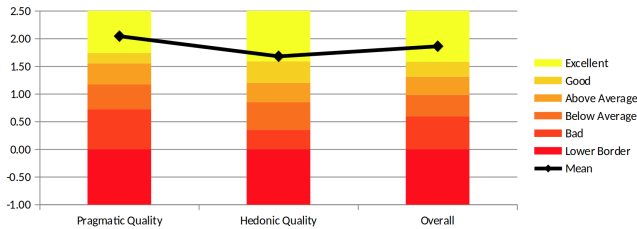
5.7.1 User Experience Questionnaire. We used the benchmarking tool of Hinderks et al. to analyze the UEQ-S and present the results for using the FIDO2 hardware key ($N = 10$) [32]. We excluded FIDO2 with Windows Hello from the analysis because a UEQ-S analysis with only one participant is ineffective.

UEQ-S contains two categories for items that describe user experience: *pragmatic*, for goal-directed aspects such as efficiency and reliability, and *hedonic*, for aspects that are not goal-directed, such as fun or novelty. For the YubiKey participants, we report a Pragmatic Quality score of 2.045 and a Hedonic Quality score of 1.682.

Table 6: Overview of experiment participants.

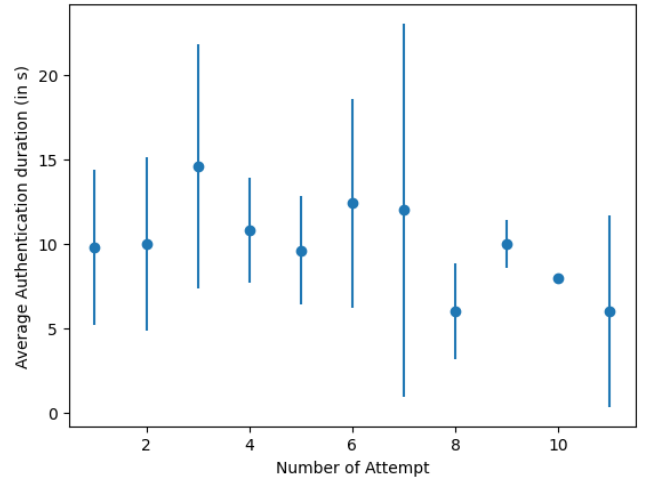
Demographics	Value	Percent
Gender:		
Female	6	54.55%
Male	5	45.45%
Age:		
20-29	1	9.09%
30-39	6	54.55%
40-49	3	27.27%
50-59	1	9.09%
Setting:		
Municipalities	7	63.64%
Refugee centers	4	36.36%
Federal State:		
Bavaria	3	27.27%
Mecklenburg-Western Pomerania	3	27.27%
Lower Saxony	2	18.18%
Hesse	2	18.18%
North Rhine-Westphalia	1	9.09%
Authentication Method:		
FIDO2 with Hardware Token	10	90.91%
FIDO2 with Windows Hello	1	9.09%
TOTP with Authenticator App	0	0.00%

As the score ranges from -3 to 3, our participants' pragmatic score is very high, indicating that the goal-directed user experience was rated highly. In contrast, the hedonic qualities were rated slightly lower, although still positive. Our findings result in an overall score of 1.864. Compared to the benchmark class provided by Hinderks et al., all scores are in the top 10% in both quality classes (cf. Figure 2). The UEQ-S benchmarking class thus postulates an excellent usability for FIDO2 with a YubiKey [32].

**Figure 2: Results of UEQ-S benchmarking class provided by Hinderks et al. [32].**

5.7.2 Semi-structured Interviews. In the following, we present the main categories from the interviews and their codes. The complete codebook can be found in the replication package (see Section A).

General Impressions and Usage of Passwordless Authentication Methods. Few participants (4) could name previously used methods in their work setting. *“It depends on how broadly that is defined. We also work with smart cards built into our computers in the city.”* The majority (7) were unaware of previous uses of passwordless authentication or were even confident that no colleagues

**Figure 3: Average time required for authentication over the number of successful authentications.**

use such a method. None of the participants could name a policy or reason for not using passwordless methods. When asked about their initial thoughts regarding passwordless authentication, three participants immediately thought of *Biometric Authentication* methods, and another three described it as something useful: *“Something very practical, so you don’t have to remember all the passwords.”*

Positive Experiences. Most participants (9) indicated they would like to continue using the method after the experiment, but even the two people who no longer wanted to use it mentioned its advantages. The main reasons for the high acceptance were the uncomplicated handling (10) and the reduced memorization effort compared to passwords (7). *“Actually, the convenience, the user-friendliness. The simplicity.”*

In addition, participants stated that they generally did not consider the method to hinder their work or that it even made their job easier (6). Another noticeable positive feature was the fun aspect of using the method (3). Thus, one participant reported: *“It’s fun. Well, it’s a bit of a technical gimmick that has always been fun. So, the haptic aspect is something that’s really, really nice.”* These impressions are backed by a visible habituation effect in the server data (Figure 3). After using the method for some time, the average authentication time went down from 10 seconds at the start of the experiment to an average of 6 seconds at the eleventh attempt.

Another useful feature of the YubiKeys was their mobility (4). Particularly in shared workplaces or home office arrangements, the possibility of using the hardware key on different devices was emphasized. *“What could be interesting is that if you carry the token, you can authenticate independently from your workplace location.”*

Problems, Barriers, and Fears. Two participants said they would not continue using the method because it offered no added value compared to the existing password login. Perceived fears while using the YubiKeys included loss (5), destruction (5), or theft (3) of the hardware keys. *“There is always the risk that I will forget, lose, or destroy the token.”*

However, multiple participants (8) directly reported coping strategies for these fears. For example, the hardware key was often attached to the key ring or deposited in a specific place in the office (safe or locker). *“So I first thought I’d put it on my keychain. But the keychain itself I can lose. And so, we have a small safe at work. And that’s where we put it.”*

Two participants also stated that they did not remove the YubiKey from the device, not even during transportation. When asked about the fear of breaking the YubiKey, a participant responded: *“During transport, yes. Because it could break if it is still plugged into the laptop.”*

For some participants, however, using the key meant a noticeable additional effort compared to the password login (3). They noted the physical effort involved in connecting the hardware key or the simplicity of the browser’s password autofill function. *“I find it relatively inconvenient that you always have to pick out this stick or token and insert it into the USB slot. For me, that is more inconvenient than entering a password.”*

Improvements. Many participants (8) did not name any possible improvements. *“In terms of process, I think, options for improvement, no, I don’t think so.”*

When explicitly asked if they would prefer the process without entering the PIN, most participants (8) indicated that they would dislike it because it would make the method feel less safe. *“Better with. Well, that’s still building on the sense of security. So I was wondering if this is 100% safe or safer than before. But this PIN creates the feeling that it is safe, after all.”*

Other than that, people commented that they would appreciate if the YubiKey were smaller (2) (*“I would prefer the dongle to be a bit smaller.”*) and if the hardware key could be used for multiple applications (1). *“It would have been cool if I could have used the method to gain access to several programs and applications at once.”*

Perception of the Method. More than half of the participants perceived the method as secure to very secure (9). In particular, they noted that the individual steps required for authentication with the YubiKey (possession of the key, PIN, and gesture with the finger) reinforced this feeling. *“It is very secure. This is only possible with this key and my PIN.”*

Regarding using YubiKeys, some participants (4) had significant misconceptions about its functionality. While the YubiKey has a haptic sensor used to detect touch motions and, thereby, the presence of a user, some participants misunderstood this as a fingerprint sensor, thereby wrongly assuming that their print was detected and that the key was personalized to them. *“Thus, I now have the key bound to my fingerprint.”*

When asked where this assumption comes from, the experiences with the smartphone were mentioned above all. Moreover, participants seemingly did not previously encounter a purely haptic sensor, so the gesture with the finger was directly connected with a fingerprint. *“Because you somehow know it from the mobile device, you just briefly hold your finger on it and no longer enter a password.”*

Passwordless Authentication in German Public Administrations. When asked whether they would support introducing passwordless authentication methods in German public administration, most participants (7) said they would, and their colleagues would probably also like it. *“The people in my department have varying*

degrees of affinity for technology, but I’m pretty sure they could all manage it somehow. I’m sure that most of them would also like it.”

As a particular benefit, introducing such authentication methods could help with the current problem with password handling. Some participants (5) reported that handling passwords within the administration is sometimes insecure, and they hope that introducing passwordless methods could improve this situation. *“Since we have not quite professionally stored our passwords [...], the risk is minimized that the passwords can be accessed somehow.”* In these cases, they commonly mentioned keeping written passwords in the office or using notebooks containing password collections. *“I have a clever little notebook [containing passwords] hidden away.”*

Some hurdles and restrictions must be considered before adoption in this domain. In the case of TOTP, problems with the required second device were mentioned (6). Many government employees do not have a work phone, and participants strongly opposed using private devices for TOTP authentication. *“For me, that wouldn’t be a big problem, but if I look across the division, you would need your private or work smartphone. However, not everyone has a work device, which would be difficult.”*

Participants (4) also pointed out the mostly inflexible and non-IT-savvy structures within the public administration, which is also related to the general mindset (3). *“I think there is still a lot that can be done regarding IT security training, both in government agencies and in general.”*

Change can thus only be achieved with external support (5) from, e.g., the respective superiors, the IT department, or political action that could influence policies. *“I don’t think that this will happen shortly. The office is still very outdated when it comes to such things. This also has much to do with an authority’s legal requirements. Even if the legal requirements allow such methods in the future, you need the will of the administrative apparatus to implement them. Even if such methods may seem fundamentally useful, it does not mean that they will be implemented in the office. So much depends on individuals at the management and political levels in a district office. If a county commissioner has a rather conservative attitude, something like this will not pass, even if possible.”*

Two participants mentioned legal regulations that might hinder the use of FIDO2. Physical YubiKeys would be considered external hardware and could only be used with separate approval and certification (1). *“But I see the problem that this is considered hardware. It’s considered external hardware; unfortunately, you can’t do that in our county yet. We still need some recognition or certificates from our IT colleagues.”* One participant noted that the devices used in their office might be too old for Hardware Security Modules (HSMs) for TPMs (1). *“I would guess that the old laptop that I still use frequently does not have the system.”*

Key Findings — In-situ Experiment. We mainly recruited younger public authority employees, but we also included employees from migrant reception centers to expand the target group. Due to the lack of availability of smartphones, restrictive workplace policies, and older work devices, the vast majority of participants used YubiKeys instead of TOTP or Windows Hello, and most would like to continue using them. Although inexperienced with passwordless authentication, participants are generally satisfied with its usability and seamless workflows.

However, they are concerned about key loss, theft, or physical damage. Participants prefer the requirement to enter a PIN, as this improves their perceived security. When confronted with specific feature descriptions from other methods, they prefer the authentication method with a YubiKey. However, introducing passwordless authentication in government bodies is described as problematic due to, e.g., restrictive policies and mindsets or workplace conditions such as a lack of work-issued phones or shared desk and device policies. The server data indicated a habituation effect, meaning participants needed less time to authenticate with the method.

6 Ethics

Scientific research with human participants always requires special care in the ethical conduct of experiments, so we took several precautions for this study. The entire study implementation and the data protection and privacy measures described below were approved by the responsible *Ethical Review Board (ERB)*. We set the configuration of the *Qualtrics* server to the maximum privacy setting for the online survey, i.e., we did not collect any metadata, such as IP addresses or user agents. However, since part of the experiment's recruitment was done via the survey, people interested in the follow-up study could voluntarily enter their contact details. In these cases, we stored their email addresses or phone numbers. Participants were also informed about the additional collection of login data and the interview audio recording for the experiment and asked for their consent. The commissioned data processing agreement also covered the collection of the login events. All data processed and collected for the experiment's realization were stored on GDPR-compliant servers in Germany and irrevocably deleted after the study. All other data, such as interview recordings, non-anonymized transcriptions, extracted log files, and contact data, never left the researcher's local device. All data was deleted after it was no longer required for this work, e.g., the audio recordings were deleted after the respective transcriptions were made. All participants completed our study voluntarily, i.e., we did not compensate them for their involvement. This partially avoided issues with federal anti-corruption laws, as participants could not accept rewards.

7 Limitations

The obtained results are limited due to the methods we used and the exploratory nature of our study. First, our work suffers from a self-selection bias, as participants participated voluntarily. Therefore, their decision to participate and our final sample might have been influenced by, e.g., their technical affinity or motivation to advance science, and our sample is therefore not generally representative [17]. Similarly, we mainly recruited via the company's network. Due to our focus on passwordless authentication and its (lack of) availability or workplace policies prohibiting using, e.g., new software and external hardware, our sample might be further biased and exclude other potentially interested participants. However, due to the scarcity of eligible participants and organizational constraints on method availability, we were unable to recruit a balanced sample for all passwordless authentication methods. However, this study aims to provide first exploratory insights into

the landscape of and sentiments towards passwordless authentication within federal institutions and not to give a representative overview of its current usage. Additionally, our survey might be influenced by common biases, such as the acquiescence bias [4, 37], i.e., participants might lean towards positive attitudes to agree with statements given within the survey, or a social desirability bias [73]. However, since the survey does not contain explicit endorsement questions, the effects of such biases are limited and more relevant for the personal assessment of passwordless authentication methods during the interview. Our experiment has a comparatively small sample size combined with the abovementioned biases. However, our main goal was to gather first insights in a qualitative and exploratory fashion. Since only little scientific work has been done on the subject so far, this work represents a first step for further research projects in the field of usable security in public authorities. It, therefore, aligns itself with the works of Farke et al., Reese et al., and Reynolds et al., who worked with similar numbers of participants and with whose help the first interesting indications for further larger research projects were discovered [19, 20, 60, 62].

8 Discussion

Below, we address our research questions and provide insights into the challenges of conducting user studies with public administration audiences in Germany. We conclude with a round-up in which we contextualize our work in the current state of research and outline our contributions.

RQ1: Participants Lacked Experience With Passwordless Authentication. Our results indicate that passwordless authentication is not widely used in German public administration. **38 (35.19%)** participants in the online survey and four out of eleven participants in the second study (cf. Section 4.3) reported being familiar with passwordless authentication. Especially in the survey, we found that TOTP was the most commonly known passwordless authentication method. However, participants experienced various issues during our experiment, leading the majority to choose YubiKeys despite prior familiarity. We assume that this disparity is based on the very individual organizational issues surrounding passwordless authentication, e.g., the current availability of company phones. Additionally, our study had an external origin and was not ordered by our participants' employers. It did not affect other software or operating systems they use. Therefore, in contrast to the previous experiences they mentioned in our surveys, participants were not directly supported and equipped. In other words, while they would receive company phones if their employer chose to adopt TOTP, they were not supplied with one for the sake of our study. As we were luckily able to provide participants with YubiKeys, they were more likely to be able to choose this option. It turns out that passwords still seem to be the dominant authentication method in this domain. The answers we received do not seem to follow any actual pattern, so it appears to be more dependent on individual IT departments whether they want to pursue the topic of secure authentication. Another interesting aspect worth noting is the mention of the home office as a reason for introducing additional authentication factors, e.g., TOTP (cf. Section 4.3.2). Therefore, the home office obligations associated with COVID-19 seem to have led to the spread of passwordless methods. However,

some participants also mention that they only need these security measures for working from home and that their office workstation is still password-protected. Hence, office devices still rely on analog security, such as physical access restrictions and password authentication.

RQ2: FIDO2 is Perceived Secure but Unorthodox. The feedback for FIDO2 methods was mainly positive, and most of the participants were eager to continue using the FIDO2 login for IG-CMS. The methods were not perceived as disruptive, and the reduced memory effort compared to passwords was highlighted (cf. Section 5.7.2). This general assessment is supported by the benchmarking UEQ-S score of 1.864 for YubiKeys. Furthermore, our participants assumed that FIDO2 authentication is generally more secure than passwords, which aligns with previous findings [19, 20, 41, 77]. However, misconceptions about YubiKey's haptic sensor could also influence perceived security. This was not evident in previous research, but it could help manufacturers, Mozilla, or Chromium optimize their User Experience and reduce misconceptions.

For the YubiKey, we encountered some known barriers, like the fear of losing, breaking, or stealing the YubiKey [20]. Participants commented that they were mostly concerned that they would lose or break the hardware key. Moreover, a few mentioned that this method had caused them extra time and effort. Contrary to the findings of Farke et al. [20], these effort barriers noted during the use were more likely to be tolerated to receive the increased security. Our experiences recruiting public sector employees (see Section 8) showed that public sector employees from Germany seem accustomed to lengthy processes and hardly notice the additional effort caused by FIDO2. The participants' reactions in the SME study by Farke et al. are sometimes much more severe (*"In the time it takes to dig it up, plug it in, enter the PIN, and push it – I could have already bought two pairs of shoes"*) [20]. That said, habituation is essential in that context. The reduction in the average time required for login, which is visible in the server data, confirms previous research [19, 20, 55] that the barriers diminish significantly as users become accustomed to new authentication procedures.

Our participants developed coping strategies against the possible loss and chose places for the token at their workplace, left it on the laptop, e.g., a key ring or office safe, or left it on the computer. Some participants mentioned they are willing to accept specific barriers for more secure methods, knowing they are working with sensitive data. According to one participant, there might be an organizational barrier to using the YubiKeys, as they could be considered an external unauthorized hardware device, which is banned in the work environment as a matter of principle for security reasons.

RQ3: Recommendations for Secure Authentication in Public Administrations. Most participants in the experiment would support the introduction of passwordless authentication methods but also foresee some hurdles (cf. Section 5.7.2). Shared desks and home offices mean no standardized and fixed workstations, and restrictive regulations make it difficult for new technologies and devices to become established. For TOTP, organizational difficulties were often mentioned due to the need for service smartphones and the lack of an authentication app in the managed app store. The positive experiences of our experiment and the quick setup of FIDO2-based methods at their workplace resulted in strong support

for this authentication scheme. However, the participants' opinions on the possible mobility of the YubiKeys were divided. On the one hand, participants who primarily work on the same device or at the same workstation found the offered mobility rather inconvenient. On the other hand, mobility is advantageous for employees who work on different computers, at home, or open workstations. If public sector organizations adopt FIDO-based authentication, this difference should be considered. Employees with fixed workplaces and devices could use a TPM setup for a more convenient use [19]. Mobile employees working from home can be equipped with hardware tokens to enable FIDO2 authentication on different devices and locations.

In addition to the end-user perspective, domain-specific challenges must be considered when deploying modern authentication methods. Our participants described inflexible structures, limited IT expertise, restrictive regulations, and hierarchical structures as specific challenges within the public sector.

The use of physical password lists instead of password managers, the low prevalence of passwordless authentication methods—only 35% of survey respondents responded that they had used one at work—and outdated security policies such as monthly password changes confirm previous research by Szczepaniuk et al. [70], which identified a lack of IT security training in public sector organizations. At least in Germany, the public sector is also very decentralized, resulting in many IT services being procured at the local level, and the respective mayor, county commissioner, or head of administration has to decide on IT changes. Departments that want to implement software changes must get approval from at least one superior and cannot independently decide on changes such as a new login method for an online service. At the same time, a whole range of legal regulations exist that hinder technological progress. The lack of authenticator apps in a managed app store, the TPM deactivation via Windows Policies, or the need for extra approval when using a YubiKey shows that IT policymakers in the public sector are not keeping up with recent developments.

Summarizing our results, we make the following recommendations to policymakers within the public sector:

- **Adoption of passwordless authentication methods:** We showed that passwords are currently the dominant authentication method, but employees can cope well with methods such as FIDO2. To increase the overall security for public services, we recommend adopting more passwordless authentication methods and considering supporting passwordless authentication, like FIDO2, as a requirement in public IT tenders.
- **Central Evaluation of IT Components:** Our findings indicate that local IT managers have difficulties keeping up to date with IT developments. To support them and streamline the verification process for public IT, we recommend introducing centralized testing and certification for software such as authenticator apps that local IT admins can incorporate.
- **Improve Security Training for End-User:** We identified some misconceptions about IT security topics. Some of these might result from outdated information (i.e., monthly password changes), but most stem from the exposure to entirely new technologies. Strong authentication is the first defense

against malicious actors, and regular trainings about recent developments improve awareness and expertise.

Researching Usable Security in German Public Administrations. Since this study seems to be the first to work with participants from the German public administration on usable and secure authentication, we provide insights into the obstacles researchers may face when working with this population. As noted in the previous sections, recruiting participants for the TOTP or TPM setup was difficult and led to lower participant numbers overall (cf. Section 5.7). This is mainly due to Germany's federal structures, which means that many decisions regarding IT systems or research projects must be discussed and settled on multiple local hierarchical levels with each municipality. While many more users of the IG-CMS were interested in participating in the experiment, participation often failed due to the organizational overhead. For example, separate application forms had to be submitted to the IT departments for individual participation, including the involvement of data protection or IT security officers with whom separate agreements had to be made. In some cases, the entire process took us up to six weeks, requiring multiple phone calls, emails, and separate agreements to obtain a single participation. Several interested individuals found the effort required to participate in a study understandably too much, so they withdrew their expressions of interest in our research.

In addition to the organizational difficulties, there were technical hurdles, which were highly individual due to the heterogeneous IT landscape of municipal administrations (cf. Section 5.7). Some devices were too old and did not have HSMs, so they could not be used as a TPM. It also appears that the TPM option can sometimes only be enabled via a Windows group policy after approval by a system operator, or that the user must set up additional MFA methods first to use the computer with a TPM. In addition, estimating the number of government employees with a service smartphone to install authenticator apps was initially challenging. Service phones are often centrally controlled with no access to the standard app stores, so users cannot install apps themselves. As a result, there was no Authenticator app available for them to use. To activate the TPM option and an Authenticator app, the participants were required to apply to the responsible IT department, which meant additional organizational effort. Our experiment involved two activation requests from December 2022 that were not processed as of December 2023. For further projects in this area, we encourage researchers to address these domain-specific problems and maybe only work with fewer municipalities, which could provide access to multiple participants at once. Hence, the organizational effort should be contained or bundled into singular requests instead of going through distinct and lengthy processes per user.

Putting Our Work Into Context. Our findings confirm several previous results [19, 20, 38, 39, 41, 60, 61]. For example, our results illustrate a similarly high acceptance of FIDO2-based methods as in previous studies [41]. We identified similar usability problems of FIDO2, such as fear of loss and destruction. Unlike previous studies, however, we did not study participants working in small companies [19, 20, 77] or universities [41]; instead, we dealt with the domain of public administration. The sheer size, complexity, federal and local regulations, and the unique characteristic of little

external pressure for change present a challenge for IT projects such as deploying novel authentication mechanisms. In light of the increasing digitization of administration and leaks, our results indicate that the usability of modern and more secure authentication methods is not the only relevant factor. On the contrary, the regulations and procedures in the domain must also be adapted so that more secure methods can be used, especially compared to other misguided security policies, guidelines, and rules that actively hinder users from using more secure methods [27].

Future Research. Our results show that end-users often do not have the opportunity to use these methods because of limitations imposed by rules and technical restrictions or the lack of support for e-government software. Therefore, subsequent research could investigate how these rules emerged, e.g., by interviewing managers responsible for public IT or manufacturers of e-government software. In addition, comparative studies with countries with a higher grade of digitization could allow further insights into this specific domain. Furthermore, a follow-up study that takes our corresponding recommendations from Section 8 into deeper consideration would be interesting. FIDO2-based methods could be examined for an entire department and, ideally, across several tools to cover the interoperability between multiple RPs. Finally, a more direct comparison between the public and private sectors would be interesting. This could be investigated using a comparative experiment between organizations from each sector.

9 Conclusion

To the best of our knowledge, we conducted the first user study focusing on passwordless authentication in public administrations in Germany. We used two research methods to investigate which assumptions employees from German public authorities have about passwordless authentication methods and how those methods are perceived. Our results show that only a minority of the participants could report experiences with these methods but that they are generally considered a practical alternative to the password. The experiment participants perceived the handling of FIDO2 as positive, and an introduction would be supported. For TOTP, technical and organizational hurdles became visible due to the lack of office smartphones or managed app stores. Considering the restrictive policies and inflexible structures, future research could investigate how the deployment of secure technologies can be made more efficient and learn more about the mental models of public employees to reduce barriers.

Acknowledgments

We thank all participants of our study and for Nicolas Huaman's support. We also would like to thank the team behind IG-CMS, especially Svenja Osmers, Daniel Kehne, and Sven Seeberg, for allowing us to use their recruiting network and support inquiries. This work was co-funded by the Volkswagen Stiftung Niedersächsisches Vorab – ZN3695 and the European Union as part of the program *Digital Europe*. Neither the European Union nor the other granting authorities can be held responsible. This work was also supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

References

- [1] Claudia Ziegler Acemyan, Philip Kortum, Jeffrey Xiong, and Dan S Wallach. 2018. 2FA might be secure, but it's not usable: A summative usability assessment of Google's two-factor authentication (2FA) methods. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 62. SAGE Publications Sage CA, Los Angeles, CA, 1141–1145.
- [2] FIDO Alliance. 2022. Apple, Google and Microsoft Commit to Expanded Support for FIDO Standard to Accelerate Availability of Passwordless Sign-Ins. <https://fidoalliance.org/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard-to-accelerate-availability-of-passwordless-sign-ins/>. Accessed: 2022-12-15.
- [3] FIDO Alliance. 2023. FIDO Authentication. <https://fidoalliance.org/fido2/>. Accessed: 2022-09-04.
- [4] Orna Baron-Epel, Giora Kaplan, Ruth Weinstein, and Manfred S Green. 2010. Extreme and acquiescence bias in a bi-ethnic population. *European Journal of Public Health* 20, 5 (2010), 543–548.
- [5] Shirley Ann Becker. 2005. E-government usability for older adults. *Commun. ACM* 48, 2 (2005), 102–104.
- [6] Nina Bindel, Cas Cremers, and Mang Zhao. 2023. FIDO2, CTAP 2.1, and WebAuthn 2: Provable security and post-quantum instantiation. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 1471–1490.
- [7] Xander Bouwman, Harm Griffioen, Jelle Egbers, Christian Doerr, Bram Klievink, and Michel van Eeten. 2020. A different Cup of TI? The Added Value of Commercial Threat Intelligence. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Online, 433–450. <https://www.usenix.org/conference/usenixsecurity20/presentation/bouwman>
- [8] Tony Bovaird and Elke Löffler. 2003. *Public management and governance*. Vol. 3. Routledge, London.
- [9] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.
- [10] Björn Bünzow. 2021. Wie organisiert man Innovation und Transformation im Föderalismus?—Digitalisierungslabore und agile Methoden als neue Formen der Zusammenarbeit. *Handbuch Onlinezugangsgesetz: Potenziale-Synergien-Herausforderungen* 1 (2021), 383–400.
- [11] Rune Bysted and Kristina Risom Jespersen. 2014. Exploring managerial mechanisms that influence innovative work behaviour: Comparing private and public employees. *Public Management Review* 16, 2 (2014), 217–241.
- [12] Åsa Cajander, Jan Gulliksen, and Inger Boivie. 2006. Management perspectives on usability in a public authority: a case study. In *Proceedings of the 4th Nordic Conference on Human-Computer Interaction: Changing Roles* (Oslo, Norway) (NordiCHI '06). Association for Computing Machinery, New York, NY, USA, 38–47. <https://doi.org/10.1145/1182475.1182480>
- [13] Victoria Clarke and Virginia Braun. 2017. Thematic analysis. *The journal of positive psychology* 12, 3 (2017), 297–298.
- [14] Department for Digital, Culture, Media & Sport. 2022. UK's Digital Strategy. <https://www.gov.uk/government/publications/uks-digital-strategy>
- [15] Alexandra Dmitrienko, Christopher Liebchen, Christian Rossow, and Ahmad-Reza Sadeghi. 2014. On the (in) security of mobile two-factor authentication. In *International Conference on Financial Cryptography and Data Security*. Springer, Berlin, Germany, 365–383.
- [16] Mohamed Hamdy Eldefrawy, Khaled Alghathbar, and Muhammad Khurram Khan. 2011. OTP-based two-factor authentication using mobile phones. In *2011 eighth international conference on information technology: new generations*. IEEE, Las Vegas, NV, USA, 327–331.
- [17] Jonas H Ellenberg. 1994. Selection bias in observational and experimental studies. *Statistics in medicine* 13, 5-7 (1994), 557–567.
- [18] Mark Evans, Ying He, Leandros Maglaras, Iryna Yevseyeva, and Helge Janicke. 2019. Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector. *International Journal of Medical Informatics* 127 (2019), 109–119. <https://doi.org/10.1016/j.ijmedinf.2019.04.019>
- [19] Florian M. Farke, Leona Lassak, Jannis Pinter, and Markus Dürmuth. 2022. Exploring User Authentication with Windows Hello in a Small Business Environment. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association, Boston, MA, 523–540. <https://www.usenix.org/conference/soups2022/presentation/farke>
- [20] Florian M. Farke, Lennart Lorenz, Theodor Schnitzler, Philipp Markert, and Markus Dürmuth. 2020. “You still use the password after all” – Exploring FIDO2 Security Keys in a Small Company. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Online, 19–35. <https://www.usenix.org/conference/soups2020/presentation/farke>
- [21] Federal Foreign Office of Germany. 2022. The Federal Government's new Digital Strategy. <https://www.auswaertiges-amt.de/en/aussenpolitik/digital-strategy/2551972>
- [22] Mary K Feeney and Leisha DeHart-Davis. 2009. Bureaucracy and public employee behavior: A case of local government. *Review of Public Personnel Administration* 29, 4 (2009), 311–326.
- [23] Daniela Fogli and Loredana Parasiliti Provenza. 2012. A meta-design approach to the development of e-government services. *Journal of Visual Languages & Computing* 23, 2 (2012), 47–62.
- [24] Asbjørn Følstad, Håvard D. Jørgensen, and John Krogstie. 2004. User involvement in e-government development projects. In *Proceedings of the Third Nordic Conference on Human-Computer Interaction* (Tampere, Finland) (NordiCHI '04). Association for Computing Machinery, New York, NY, USA, 217–224. <https://doi.org/10.1145/1028014.1028047>
- [25] Lorenzo Franceschi-Bicchiera. 2023. CISA says US government agency was hacked thanks to 'end of life' software. <https://techcrunch.com/2023/12/06/cisa-says-us-government-agency-was-hacked-thanks-to-end-of-life-software/>
- [26] Lorenzo Franceschi-Bicchiera. 2023. Cyber attack on British Library raises concerns over lack of UK resilience. <https://www.ft.com/content/642ee014-4768-4c65-b1ee-0d4f39a8a63d>
- [27] Eva Gerlitz, Maximilian Häring, and Matthew Smith. 2021. Please do not use !?_ or your License Plate Number: Analyzing Password Policies in German Companies. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, Online, 17–36. <https://www.usenix.org/conference/soups2021/presentation/gerlitz>
- [28] Government of Canada. 2022. Canada's Digital Ambition. <https://www.canada.ca/en/government/system/digital-government/government-canada-digital-operations-strategic-plans/canada-digital-ambition.html>
- [29] Paul A Grassi, Michael E Garcia, and James L Fenton. 2017. Digital identity guidelines. *NIST special publication* 800 (2017), 63–3.
- [30] Morey J Haber. 2020. *Passwordless authentication*. Apress, Berkeley, CA, 87–98.
- [31] Eszter Hargittai and Yuli Patrick Hsieh. 2012. Succinct Survey Measures of Web-Use Skills. *Social Science Computer Review* 30, 1 (2012), 95–107. <https://doi.org/10.1177/0894439310397146> arXiv:https://doi.org/10.1177/0894439310397146
- [32] Andreas Hinderks, Martin Schrepp, and Jörg Thomaschewski. 2018. *A Benchmark for the Short Version of the User Experience Questionnaire*. SCITEPRESS, Setubal, Portugal, 373–377.
- [33] Michael Jones. 2020. CBOR Object Signing and Encryption (COSE) and JSON Object Signing and Encryption (JOSE) Registrations for Web Authentication (WebAuthn) Algorithms. RFC 8812. <https://doi.org/10.17487/RFC8812>
- [34] Mark Keith, Benjamin Shao, and Paul John Steinbart. 2007. The Usability of Passphrases for Authentication: An Empirical Field Study. *International journal of human-computer studies* 65, 1 (2007), 17–28.
- [35] Agata Kruzikova, Lenka Knapova, David Smahel, Lenka Dedkova, and Vashek Matyas. 2022. Usable and secure? User perception of four authentication methods for mobile banking. *Computers & Security* 115 (2022), 102603.
- [36] Dhruv Kuchhal, Muhammad Saad, Adam Oest, and Frank Li. 2023. Evaluating the Security Posture of Real-World FIDO2 Deployments. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (Copenhagen, Denmark) (CCS '23). Association for Computing Machinery, New York, NY, USA, 2381–2395. <https://doi.org/10.1145/3576915.3623063>
- [37] Ozan Kuru and Josh Pasek. 2016. Improving social media measurement in surveys: Avoiding acquiescence bias in Facebook research. *Computers in Human Behavior* 57 (2016), 82–92.
- [38] Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. 2021. "It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Copenhagen, Denmark, 91–108. <https://www.usenix.org/conference/usenixsecurity21/presentation/lassak>
- [39] Leona Lassak, Elleen Pan, Blase Ur, and Maximilian Golla. 2024. Why Aren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication. In *33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association, Philadelphia, PA, 7231–7248. <https://www.usenix.org/conference/usenixsecurity24/presentation/lassak>
- [40] Bettina Laugwitz, Ulf Schubert, Waltraud Ilmberger, Nina Tamm, Theo Held, and Martin Schrepp. 2009. Subjektive Benutzerzufriedenheit quantitativ erfassen: Erfahrungen mit dem User Experience Questionnaire UEQ. In *Tagungsband UP09. Tagungsband UP09* 9, 220–225.
- [41] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. 2020. Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. In *IEEE Symposium on Security and Privacy*. IEEE, Online, 268–285.
- [42] Sean Lyngaas. 2023. Exclusive: US government agencies hit in global cyberattack. <https://edition.cnn.com/2023/06/15/politics/us-government-hit-cyberattack/index.html>
- [43] Karola Marky, Kirill Ragozin, George Chernyshov, Andrii Matvienko, Martin Schmitz, Max Mühlhäuser, Chloe Eghtebes, and Kai Kunze. 2022. "Nah, it's just annoying!" A Deep Dive into User Perceptions of Two-Factor Authentication. *ACM Trans. Comput.-Hum. Interact.* 29, 5, Article 43 (10 2022), 32 pages. <https://doi.org/10.1145/3503514>
- [44] Peter Maxwell, Martin Vornweg, and Yasemin Yuecksel. 2022. Landkreis Anhalt-Bitterfeld, you are fucked. <https://www.spiegel.de/panorama/cybercrime-wie-hacker-den-landkreis-anhalt-bitterfeld-lahmlegten-podcast-a-9572cbea-2404-4a5d-9db4-b718d1c6d9d4>

- [45] Patrick McDaniel and Farinaz Koushanfar. 2023. Secure and Trustworthy Computing 2.0 Vision Statement. arXiv:2308.00623 [cs.CR]
- [46] Allison McDonald, Catherine Barwulor, Michelle L. Mazurek, Florian Schaub, and Elissa M. Redmiles. 2021. "It's stressful having all these phones": Investigating Sex Workers' Safety Goals, Risks, and Practices Online. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Online, 375–392. <https://www.usenix.org/conference/usenixsecurity21/presentation/mcdonald>
- [47] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *ACM on Human-Computer Interaction* 3, CSCW, Article 72 (2019), 23 pages.
- [48] Craig Metz. 1997. OTP Extended Responses. RFC 2243. <https://doi.org/10.17487/RFC2243>
- [49] Thomas Meuche. 2022. Dilemmata und Wege zur Digitalisierung der öffentlichen Verwaltung. *Gruppe. Interaktion. Organisation. Zeitschrift für Angewandte Organisationspsychologie (GIO)* 53, 1 (2022), 99–108.
- [50] David M'Raihi, Salah Machani, Mingliang Pei, and Johan Rydell. 2011. *Totp: Time-based one-time password algorithm*. Technical Report. Internet Engineering Task Force (IETF).
- [51] David M'Raihi, Johan Rydell, Mingliang Pei, and Salah Machani. 2011. TOTP: Time-Based One-Time Password Algorithm. RFC 6238. <https://doi.org/10.17487/RFC6238>
- [52] Next:Public Beratungsagentur. 2021. Verwaltung in Krisenzeiten 2. <https://nextpublic.de/verwaltung-in-krisenzeiten-2/>. Accessed: 2024-11-29.
- [53] Volker Nissen, Frank Termer, Mathias Petsch, Thomas Müllerleile, and Matthias Koch. 2017. *Aufgaben und Anforderungen an den CIO—ein Vergleich zwischen Privatwirtschaft und öffentlicher Verwaltung*. Springer, Wiesbaden, Germany, 211–225. https://doi.org/10.1007/978-3-658-13760-1_16
- [54] Government of Canada. 2023. BGRS and SIRVA Canada systems privacy breach affecting current and former federal employees. <https://www.canada.ca/en/government/system/digital-government/online-security-privacy/bgrs-sirva-canada-systems-privacy-breach-affecting-current-former-federal-employees.html>. Accessed: 2024-01-15.
- [55] Kentrell Owens, Olabode Anise, Amanda Krauss, and Blase Ur. 2021. User Perceptions of the Usability and Security of Smartphones as FIDO2 Roaming Authenticators. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, Online, 57–76. <https://www.usenix.org/conference/soups2021/presentation/owens>
- [56] Surjit Paul and Saini Das. 2020. Accessibility and usability analysis of Indian eGovernment websites. *Universal Access in the Information Society* 19, 4 (2020), 949–957.
- [57] Thanasis Petsas, Giorgos Tsirantonakis, Elias Athanasopoulos, and Sotiris Ioannidis. 2015. Two-factor authentication: is the world ready? quantifying 2FA adoption. In *Proceedings of the Eighth European Workshop on System Security (Bordeaux, France) (EuroSec '15)*. Association for Computing Machinery, New York, NY, USA, Article 4, 7 pages. <https://doi.org/10.1145/2751323.2751327>
- [58] Manuela Preoteasa. 2023. The Federal Government's new Digital Strategy. <https://www.euractiv.com/section/digital/news/romania-new-government-vows-to-speed-up-digital-transformation/>
- [59] Ashwini Rao, Birendra Jha, and Gananand Kini. 2013. Effect of grammar on security of long passwords. In *Proceedings of the Third ACM Conference on Data and Application Security and Privacy (San Antonio, Texas, USA) (CODASPY '13)*. Association for Computing Machinery, New York, NY, USA, 317–324. <https://doi.org/10.1145/2435349.2435395>
- [60] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. 2019. A Usability Study of Five Two-Factor Authentication Methods. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 357–370. <https://www.usenix.org/conference/soups2019/presentation/reese>
- [61] Kendall R. Reese. 2018. *Evaluating the Usability of Two-factor Authentication*. Ph.D. Dissertation. Brigham Young University. <https://www.proquest.com/dissertations-theses/evaluating-usability-two-factor-authentication/docview/2442264496/se-2> Copyright - Database copyright ProQuest LLC; ProQuest does not claim copyright in the individual underlying works; Last updated - 2024-07-18.
- [62] Joshua Reynolds, Trevor Smith, Ken Reese, Luke Dickinson, Scott Ruoti, and Kent Seamons. 2018. A Tale of Two Studies: The Best and Worst of YubiKey Usability. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 872–888. <https://doi.org/10.1109/SP.2018.00067>
- [63] Michael Richards. 2023. No Time to Waste: Government IT Modernization Must Take Off Now. <https://www.uschamber.com/technology/no-time-to-waste-government-it-modernization-must-take-off-now>
- [64] Shannon Riley. 2006. Password security: What users know and what they actually do. *Usability News* 8, 1 (2006), 2833–2836.
- [65] Benjamin Saunders, Julius Sim, Tom Kingstone, Shula Baker, Jackie Waterfield, Bernadette Bartlam, Heather Burroughs, and Clare Jinks. 2018. Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & quantity* 52 (2018), 1893–1907.
- [66] Martin Schrepp, Andreas Hinderks, and Jörg Thomaschewski. 2017. Design and evaluation of a short version of the user experience questionnaire (UEQ-S). *International Journal of Interactive Multimedia and Artificial Intelligence*, 4 (6), 103–108, 6, 4 (2017), 103–108.
- [67] Martin Schrepp, Jörg Thomaschewski, and Andreas Hinderks. 2017. Construction of a benchmark for the user experience questionnaire (UEQ). *International Journal of Interactive Multimedia and Artificial Intelligence* 4, 4 (2017), 40–44.
- [68] Richard Shay, Saranga Komanduri, Adam L. Durity, Phillip Huh, Michelle L. Mazurek, Sean M. Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2014. Can long passwords be secure and usable?. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 2927–2936.
- [69] Trui Steen and Carina Schott. 2019. Public sector employees in a challenging work environment. *Public Administration* 97, 1 (2019), 3–10.
- [70] Edyta Karolina Szczepaniuk, Hubert Szczepaniuk, Tomasz Rokicki, and Bogdan Klepacki. 2020. Information security assessment in public administration. *Computers & Security* 90 (2020), 101709. <https://doi.org/10.1016/j.cose.2019.101709>
- [71] Viktor Taneski, Marjan Heričko, and Boštjan Brumen. 2019. Systematic overview of password security problems. *Acta Polytechnica Hungarica* 16, 3 (2019), 143–165.
- [72] Kurt Thomas, Frank Li, Ali Zand, Jacob Barrett, Juri Ranieri, Luca Invernizzi, Yarik Markov, Oxana Comanescu, Vijay Eranti, Angelica Moscicki, et al. 2017. Data breaches, phishing, or malware? Understanding the risks of stolen credentials. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*. Association for Computing Machinery, New York, NY, USA, 1421–1434.
- [73] Thea F Van de Mortel. 2008. Faking it: social desirability response bias in self-report research. *Australian Journal of Advanced Nursing*, The 25, 4 (2008), 40–48.
- [74] Rafael Veras, Christopher Collins, and Julie Thorpe. 2014. On semantic patterns of passwords and their security impact.. In *NDSS*. Internet Society, San Diego, CA, USA, 1–16.
- [75] Silas Formunyuy Verkijika and Lizette De Wet. 2018. A usability assessment of e-government websites in Sub-Saharan Africa. *International Journal of Information Management* 39 (2018), 20–29.
- [76] Karen Werner. 2020. Uni Gießen: So teuer war der Hackerangriff wirklich. <https://www.giessener-allgemeine.de/giessen/uni-giessen-hackerangriff-kosten-iliias-90015054.html>
- [77] Leon Würsching, Florentin Putz, Steffen Haesler, and Matthias Hollick. 2023. FIDO2 the Rescue? Platform vs. Roaming Authentication on Smartphones. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (Hamburg, Germany) (CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 68, 16 pages. <https://doi.org/10.1145/3544548.3580993>

A Availability

All used materials are available at the following Open Society Foundation repository: doi.org/10.17605/OSF.IO/9TJD2

Documents are available in English and German and include the online survey, recruitment emails, codebooks (Survey & Experiment), the interview guide, and used translations.

B Background

In this section, we present background information on covered passwordless authentication mechanisms. Methods classified as Passwordless Authentication are usually described as procedures that do not require combining username and password but use other authentication factors [43]. There have been several efforts to introduce new methods since the usage of classic passwords entails several technical and human security problems [59, 64, 68, 71, 72, 74].

B.1 Authentication with FIDO2

FIDO2 is developed by the FIDO Alliance and the W3C [2]. As their previous standard U2F failed, the FIDO2 authentication protocol was introduced to replace passwords as the predominant login method [41]. The protocol is based on the WebAuthn authentication standard and the updated CTAP2 protocol [33].

Figure 4 illustrates the interaction of the two procedures and the location of the components required in a FIDO2 authentication process. For FIDO2, users need a private key and an associated

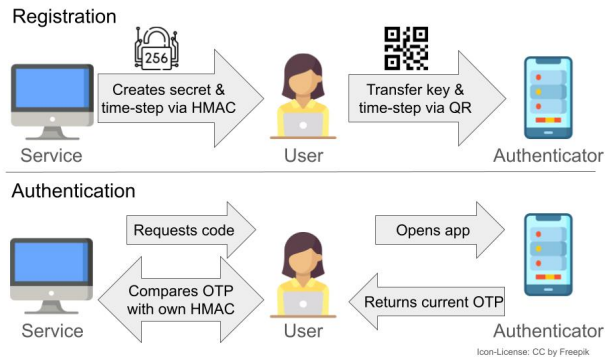


Figure 5: An illustration of the TOTP process.

public key known to the Relying Parties (RP) with which authentication will be performed. The private key is required first for the generation and subsequent registration of a key pair via FIDO2. The key can be stored on an external hardware device (Roaming Token) or an embedded Hardware Security Module (HSM) chip. CTAP2 specifies how the client interacts with the device on which the private key is located and defines the methods (like register, challenge, and assert) that the client can issue to the authenticator. Third parties can now send authentication challenges to the client using the known public key via the WebAuthn. The challenge is passed on to CTAP2 and can be validated using the private key. All major browsers support this standard and provide a channel where RPs can interact with clients using the same methods. This entire interaction between a third party and the authenticator is called FIDO2 [60].

B.2 Authentication with TOTP

TOTP is based on the procedure for generating one-time passwords but adds a temporal component as an additional security mechanism. One-time passwords (OTP) are valid only once and invalidated after use. This procedure is widespread, e.g., for online banking, where printed or device-based transaction authentication numbers (TANs) were used [35, 48]. Newer methods, however, tend to rely on smartphone-based procedures by sending codes via SMS or through a separate app [35].

An additional time component is added if the method is extended to TOTP. After the authentication service has formed the OTP, a time window is formed during which the code is valid. This can happen via timestamps or dynamic generation of codes, which occurs without a static time window. Procedures via apps are becoming more widespread and more secure than SMS-based procedures [16, 50]. Figure 5 displays an abstract view of an app-based procedure [51, 60].

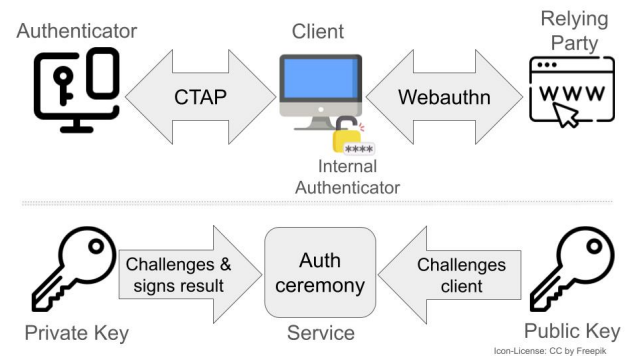


Figure 4: Illustrating a FIDO2 authentication process.