Investigating Verification Behavior and Perceptions of Visual Digital Certificates

Dañiel Gerhardt and Alexander Ponticello, *CISPA Helmholtz Center for Information Security and Saarland University;* Adrian Dabrowski and Katharina Krombholz, *CISPA Helmholtz Center for Information Security*

Investigating Verification Behavior and Perceptions of Visual Digital Certificates

Dañiel Gerhardt*
CISPA Helmholtz Center for Information Security and Saarland University

Alexander Ponticello*
CISPA Helmholtz Center for Information Security and Saarland University

Adrian Dabrowski
CISPA Helmholtz Center for Information Security

Katharina Krombholz
CISPA Helmholtz Center for Information Security

Abstract

This paper presents a qualitative study to explore how individuals perceive and verify visual digital certificates with QR codes. During the COVID-19 pandemic, such certificates have been used in the EU to provide standardized proof of vaccination.

We conducted semi-structured interviews with $N = 17$ participants responsible for verifying COVID-19 certificates as part of their job. Using a two-fold thematic analysis approach, we, among other things, identified and classified multiple behavioral patterns, including inadequate reliance on visual cues as a proxy for proper digital verification.

We present design and structural recommendations based on our findings, including conceptual changes and improvements to storage and verification apps to limit shortcut opportunities. Our empirical findings are hence essential to improve the usability, robustness, and effectiveness of visual digital certificates and their verification.

1 Introduction

Barcodes are a visual yet machine-readable representation of data. Historically, barcodes held very little data, merely representing a link to an external database (e.g., an article id, parcel tracking number, concert tickets) or an external resource (e.g., URL). Thus, many barcode-based solutions, such as concert tickets, rely on online verification or employ hard-to-forge physical security measures, similar to passports [28].

Visual digital certificates can be (i) more privacy-preserving since data is only processed locally, (ii) distributed rapidly as no central authority needs to manufacture forge-resistant prints, (iii) more sustainable and cost-efficient as users do not need to print them or can do so at home, and (iv) more robust against forgery. They facilitate high-density barcodes holding authoritative data secured by a digital signature. So far, they have not been widely used in state-issued (but not state-printed) certificates, passes, or other documents.
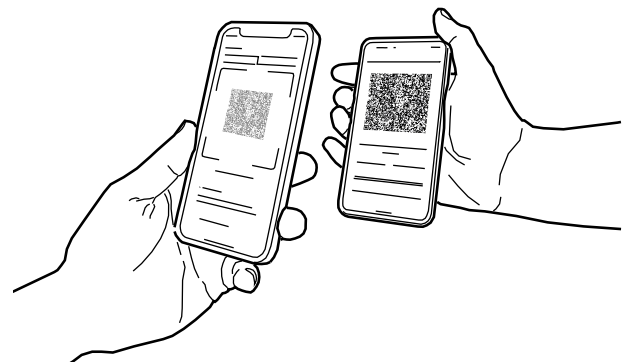

Figure 1: A *verifier* scanning the vaccination data of an EU-DCC *certificate holder*.

Soon after the COVID-19 pandemic was declared by the WHO [53], many countries recognized the need to impose limits on travel and entrance to public places based on vaccination, recovery, or testing status [9, 10]. In order to check the status of a person, the European Union coordinated development efforts on a standardized digital certificate, the EU Digital COVID Certificate (EUDCC) [12]. Subsequently, the EUDCC became the largest rollout of offline-verifiable state-issued visual digital certificates to date. That is a digitally-signed document usually presented in the form of a QR code on a digital medium or in printed form. In order to verify such a certificate, a person has to scan the QR code via an appropriate app (see Figure 1 and Section 2) to verify the signature. Then the *verifier* needs to cross-check the certificate holder's identity using a legal ID.

However, this measure can only be effective if the verification procedure is performed correctly. Anecdotal evidence from news articles [26, 49, 51] as well as the authors' personal experiences, suggest that certificates are often insufficiently or incorrectly verified. Verifiers would often merely look at certificates without scanning the QR code, fail to cross-check the holder's identity via a picture ID, or simply not perform any verification at all. These insufficient verification procedures undermine the theoretical security guarantees of visual

---

digital certificates such as the EUDCC, and open the door for malicious actors to use counterfeits and wrongfully claim received vaccinations or negative tests.

Previous work [24, 36, 39] has demonstrated how users' perceptions of a system influence their (insecure) usage, and highlighted the importance of understanding users' knowledge about technical systems in order to provide them with solutions they can use securely. In the context of COVID-19, previous work has studied users' perceptions about contact tracing apps and their willingness to use them [27], investigated worldwide deployment and proliferation of digital vaccination and testing certificates [30, 38], evaluated technical, legal, and ethical implications of various proposed solutions for digital vaccination certificates [37], developed decentralized, privacy-preserving solutions for offline-verifiable certificates [19], and explored user perceptions of vaccination certificates from the holders' perspective [31].

However, to our knowledge, this is the first paper investigating visual digital certificates from the verifier's perspective. In particular, we show how they are processed in the wild and elicit verifiers' understanding of the underlying security concepts. We conducted a qualitative study with $N = 17$ professionals responsible for regularly checking vaccination certificates as part of their jobs. During semi-structured interviews, we presented participants with three scenarios and asked them to verify the EUDCCs of fictionalized customers.

We evaluated our data using a thematic analysis approach [8] with regard to participants' verification behavior and their understanding of the underlying system.

This paper provides the following four contributions:

(1) detailed descriptions of the building blocks constituting verification processes in the wild,

(2) findings on behavioral patterns that can be classified as four distinct types of verification behavior,

(3) insights into users, i.e., verifiers' perceptions of the system with regard to threat models, and

(4) implications for the design of visual digital certificates as well as directions for future research.

The study, therefore, advances security and privacy efforts related to visual digital certificates. User authentication, cryptographic methods' usability, and private data handling are core security and privacy research topics. As new applications for digital visual certificates are discussed (e.g., digital driver's licenses [52]), it becomes essential to understand the implications and perspective of the enforcing personnel. The security and other goals of this and future deployments can only be met with the correct application of the verification procedure.

2 Background

The EUDCC, colloquially *green pass*, is the largest rollout of a new generation of offline-verifiable state-issued but not state-

printed authentication documents, certificates, and passes. Instead of relying on hard-to-forge physical security measures, these documents contain (or entirely consist of) a digitally-signed QR code. In the case of the EUDCC, these certificates attest to a specific testing, recovery, or vaccination status to enforce pandemic-induced limitations on travel and admission. The effectiveness of such QR code-based certificates –current and any new future uses– heavily relies on correct verification by the enforcing personnel. Throughout this paper, we use the following terminology to refer to the people involved in the EUDCC verification process:

Certificate holder refers to the person who owns the certificate and presents it in the process of requesting admission to a certain venue (e.g., gym, bar). In the context of this work, *customer* and *presenter* are synonyms for a certificate holder.

Verifier refers to the person responsible for checking a certificate. We focus on individuals who have to verify certificates as part of their daily job routine (e.g., waiters, bouncers). We use the term *verifier* in accordance with the relevant legal documents and technical specification [18, 20]. Technically, this role performs both verification of the signature as well as validation of the vaccination certificate according to the respective rules applying to their work environment.

2.1 EUDCC Verification

The verification procedure (depicted in Figure 2) is equivalent for both the paper and digital version of the EUDCC, as specified by the eHealth Network's technical specification [18]. First, the *certificate holder*, requests admission to an entry-restricted venue. An authorized staff member of that venue, the *verifier*, is responsible for checking the holder's certificate and granting access based on the current state legislation or private venue rules. Therefore, the certificate holder presents the proper EUDCC. The verifier uses any authorized verification app on a compatible device to scan the QR code containing the digital certificate. Then, the verifier obtains the name and date of birth (DoB) from the scanned certificate, while disregarding any of the information included along the QR code on the paper or application used to display the EUDCC. To tie the EUDCC to a person, they then demand a legal photo ID (e.g., passport, state-issued picture ID, driving license) and verify the identity of the person by matching the name and date of birth to the certificate and the picture to the person. If all steps are completed, the verifier decides on admission based on the status (e.g., testing, vaccination, and elapsed time).

2.2 EUDCC Apps in Germany

We conducted our study in Germany, where several applications exist to present and verify the EUDCC. The two most popular apps for storing digital COVID certificates are Cov-Pass [44] and Corona-Warn-App [42]. Both applications are
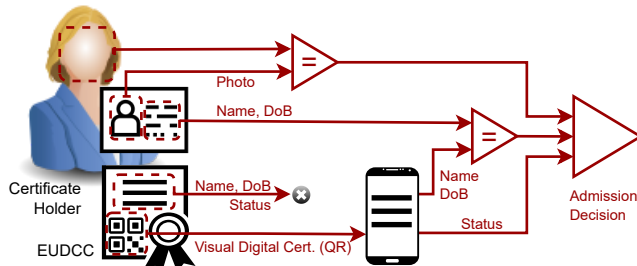
Figure 2: Correct EUDCC verification process. Note: human-readable data from the certificate must not be used, even if provided.

open-source projects. They can hold multiple certificates and display the contents of each EUDCC as a QR code and in human-readable form. The latter is intended for the certificate holder but not for verification purposes [12, 44]. Notable updates for both apps, introduced in late 2021 [1, 2], added a warning stating that the QR code needs verification with an appropriate app. Since February 2022, there has been a limit on the number of certificates that can be stored to prevent misuse [3].

The most popular verifier app is CovPassCheck [45]. This publicly available app allows scanning and verifying the EUDCC offline, i.e., without an active internet connection. The app only occasionally needs to download the necessary checking rules and key signature material from the national backend [17]. Starting with version 1.17, the app included a feature for validating certificates under a variety of legal regulations. Before this update, verifiers had to manually check a customer's vaccination count to determine compliance with legal requirements [4].

3 Related Work

We summarize previous work about user understanding and decision making in the context of security, demonstrating the importance of investigating end-users' understanding and how this leads to different security behavior. We also discuss work on digital vaccination certificates focusing on end-users and the technical implementation of the technology.

The presented related works below show the technical feasibility, end-users' willingness for adoption, and how bad security practices can be reduced. However, they do not answer why people commonly perform incorrect verification, which involves decision making influenced by their understanding of the technology.

3.1 User Understanding and Decision Making in Security

Research on users' understanding of security and how it affects their response to certain risks demonstrates that it is

helpful to build an understanding of certain technologies in end-users with appropriate risk communication to promote safer decision making. However, technical education alone is not sufficient. Policies and respective systems should ensure security for these users. Previous work has shown that users' understanding plays an essential role in their security-relevant decision making in other contexts such as browsing the web or casting and verifying votes in the digital space. However, related work mostly considered non-professional users, making predominantly passive decisions. In contrast, we investigate the professional verifiers' side, which requires conscious decision making. Our goal is to identify the perceptions and understanding that influence the verifiers' decision making, specifically in our context.

Camp [11] highlights that although security concerns have been steadily increasing, security tools are not widely used. Specifically, in computer security, this can lead to inadequate risk perception due to ineffective risk communication. Camp concluded that using suitable mental models to communicate risks in different situations is essential and can improve risk communication if used correctly.

Spero et al. [48] reviewed cognitive science and cybersecurity literature to show that UI design inhibits mental models by concealing most of the security-relevant aspects of software functionality. This impairs users' ability to detect threats and take appropriate measures to protect themselves. The authors conclude that accurate mental models are required to guide secure actions.

Zollinger et al. [54] developed a mobile application for vote-casting and vote-verification with a more user-oriented design than past solutions and tested their interface in interviews with 38 participants to collect user experience data. They found that an understanding of the verification phase has to be facilitated as users are not aware of the purpose of the verification. The authors concluded that an easy-to-perform verification mechanism is helpful but not sufficient to convince users of the security behind the system.

A qualitative study by Stojmenović et al. [50] investigated non-expert users' mental models of website certificates. They tested an interactive interface designed for building mental models of web certificates with the goal of alleviating the lack of mental models these users have. After the 21 participants used the interface, they exhibited increased trust in websites with Extended Validation (EV) certificates while demonstrating lower trust in websites without such certificates. This lead to safer decisions online.

Previous work in the domain of users' understanding of security on the internet has come to different conclusions about how individuals' internet knowledge affects their security decisions. Kang et al. [29] explored this further to determine how certain knowledge affects users' responses to potential risks by conducting a qualitative study with technical and non-technical participants. They reported that while participants with different technical education or experience showed dif-

ferent mental models of how the internet works, these factors were mostly not predictive of their behavior regarding their own security. The authors suggest emphasizing on policies and systems that protect security without relying too much on users' security practices.

3.2 COVID-19 Digital Vaccination Certificate

Before the EUDCC rollout, prototypes and studies had been used to test the feasibility of digital vaccination certificates.

User preferences of COVID vaccination certificates were studied with 599 participants in Germany by Kowalewski et al. [31] in an online study conducted prior to the EUDCC rollout in July 2021. They investigated five paper-based and app-based designs, including one similar to the official app-based solution deployed at the time of writing. The results indicate that, in general, the willingness to use and utility of vaccination certificates were perceived positively with a preference for paper-based solutions. It is important to note that this is the certificate holders' preference, whereas the perspective of the certificate verifiers was not the focus of this paper.

Eisenstadt et al. [19] built a proof-of-concept mobile phone app and server architecture to demonstrate the feasibility of digital vaccination certificates. The solution allowed the end-user to present a vaccination certificate while not revealing other personal information. Although the EUDCC is implemented differently, their work demonstrated the general feasibility of the technology.

4 Methodology

Anecdotal evidence [26, 49, 51] suggests that the verification process of digital COVID certificates is often done insufficiently. Since a correct verification process is crucial for the security of any system relying on visual digital certificates, and previous research [24, 36, 39] has demonstrated the importance of understanding users' perceptions about a system for a secure behavior, we sought to close an important gap in the literature by answering the following research questions:

RQ1 How do professional[1] users verify the EUDCC?

RQ2 What understanding do professional users have of the underlying verification process of the EUDCC?

Due to the nature of our research questions, we followed an inductive exploratory approach and conducted semi-structured interviews that we later analyzed using thematic analysis. Similar approaches have been used by previous work [5, 39] to investigate users' understanding of technical systems as well as investigate formerly unexplored topics without requiring a

---
[1]*Professional* refers to individuals who verify vaccination certificates as part of their duties at work

pre-established theory. In the following, we provide details on data collection and analysis.

4.1 Interview Structure and Procedure

To start, we briefed the participants about the topic of the study and how their data was going to be handled. As presented in the interview guideline (see Appendix A), the interview consists of three main parts plus a final demographic questionnaire. For the first part, we asked participants a series of warm-up questions about their current job, such as how often they typically verify an EUDCC during a working day. The second part consists of three different scenarios in a set order. Each scenario consists of a fictionalized person, who requests access to the participant's venue. To do so, the person presents a digital COVID certificate. We asked our participants to perform verification as they would do in real life. To further enhance the immersion, we presented them with a portrait of the fictionalized customer, for whom we also prepared a fabricated ID. The interviewer would present this ID upon request, reflecting common real-world behavior. Previous work has shown that scenarios are a useful and effective tool for understanding users' perceptions of a system [6, 32, 39]. We observed how participants evaluated the certificates in each scenario and took notes on their behavior.

We conducted interviews between December 2021 and May 2022. Due to the ongoing COVID-19 pandemic most of them (15/17) took place online over video call. For the two in-person interviews we presented the scenario materials (certificates, pictures, IDs) on a smartphone or in printed-out form on paper. For the online interviews, we created HTML Image Maps to mimic the interaction with a physical device (see Appendix C). The interviewer presented the scenarios via screen sharing and enabled remote control for participants. Finally, we asked participants to summarize the whole process of verifying EUDCCs. We furthermore collected data about their concrete understanding of the verification process of the EUDCC by inquiring about potential attack vectors they can come up with, as well as how and where they learned about the process.

Following the interview, we gave participants the chance to ask any remaining questions. Afterward, we explained the correct verification process to them if they lacked sufficient understanding. Finally, we explained the purpose and motivation for the study.

Scenarios The three scenarios and the order in which we presented them were designed to encourage participants to share a large amount of their perceptions and understanding. We achieved this by varying the familiarity of the UI, the information visible on the certificates, as well as including an analog certificate. This made it more likely that the participants would talk about different aspects of their understanding instead of focusing on one for all three scenarios. The scenarios cover both digital and analog modes of the EUDCC. For

the former, we chose to use a well-known application (the German CovPass app [44]) as well as an alternative UI we constructed such that participants would not have been able to encounter it prior to the study.

For each scenario, we constructed a fictionalized person by combining the personally identifiable information (PII) from the respective certificate with an AI-generated picture. Participants can see the picture alongside the certificate. This detail is crucial since a complete verification includes matching the certificate to the holder (i.e., by cross-checking personal details with an official photo ID). For each person, we create a matching ID card, which we would show participants upon request during the verification process. We used real and valid certificates to maximize ecological validity since self-generated certificates would not be accepted by an official verification app, which our participants used at work. These certificates were thankfully provided to us by friends and family members who gave us their explicit consent to use the certificates for our study after we explained the study design in detail.

While medical data is generally sensitive, the information provided through the certificate is regularly presented when visiting an access-restricted facility.

To further protect the identity of the original certificate holders in the scenarios, we used an AI-generated picture instead of the actual photo, as well as fabricated IDs. These IDs included the real name and date of birth, matching the data in the certificates, along with fabricated information such as picture, ID number, place of birth, and expiration date. See Figure 4d in Appendix C for an example. After the interview, we explained to participants who had stored a certificate persistently that their behavior violates people's privacy.

1. CovPass The first scenario (see Figure 4a in Appendix C) includes the EUDCC stored with the CovPass app from the German public health institute (Robert Koch-Institut) [44]. We chose this application since it appears to be the most widespread one in Germany for this purpose. While there are no public numbers on the number of active users, as of October 2022, the app has over 107,000 reviews and 10 million downloads on the Google Play store [43] which points to a significant user base considering Germany's total population of around 84.0 million [23]. We, therefore, assume that most participants are familiar with this interface so that they can share their basic understanding of the verification process. The certificate is presented by a young man. For the online interviews, we recreated the interface allowing full interaction and mimicking the CovPass app. Participants can navigate to sub-menus to reveal detailed information about the certificate.

2. Obscure UI The second scenario (Figure 4b in Appendix C) is also presented on a smartphone and consists of a QR code embedded into an obscure UI, specifically chosen to be unfamiliar. The certificate is shown as part of a custom-made digital pass with a black background and some text that does not contain any relevant information, like the name of the certificate holder or date of vaccination. We used Apple Wallet, which allows custom-made passes but has a neutral UI otherwise. Furthermore, the app does not provide any additional interaction, thus prohibiting participants from verifying personal information manually. We included this scenario to understand participants' perceptions more precisely as they are still being presented with a valid certificate. Still, they cannot rely on data displayed on-screen or interaction with the certificate for verification. The certificate is presented by a middle-aged woman.

3. Paper The third scenario (Figure 4c in Appendix C) includes a printed version of the EUDCC on paper. We expected most participants to be familiar with this document, as most people in Germany will receive their certificate in this form upon getting vaccinated [22]. It can serve as an analog replacement for, e.g., less tech-savvy users or individuals without smartphones. The third scenario is similar to the first scenario in the information shown and the familiarity to most users. It is distinct by the physical form factor as opposed to the digital certificate. The certificate is presented by a young woman. The online version allows the participant to zoom in on different document areas.

We presented the scenarios in this order to get a thorough picture of the participants' perceptions. We chose to present the most prevalent scenario first to get a basic understanding of the verification process and give participants an easy start. We followed up with the obscure scenario to challenge participants and get them out of their comfort zone. The final scenario covers certificates that are not presented on a smartphone to get insights into whether participants would perform a different verification based on the form factor. While going through the scenarios, we asked participants to verify each certificate as they would do at their workplace. We also encouraged them to explain their thought process in as much detail as possible and asked follow-up questions.

Pilot Interviews We validated our interview setup with two pilot interviews done remotely. Based on the results, we implemented the following changes to the interview guideline: Initially, we did not include pictures of the person presenting the certificate. To make scenarios more realistic, we showed the face of the fictional certificate holder alongside the certificate after the first pilot interview. We furthermore made minor adjustments to the demographics form. Specifically, we opted to ask the question about digital signature knowledge verbally rather than in the survey such that we could clarify any misunderstandings participants had with the question. The pilot study also confirmed our initial expectations for the interview's duration to be around 30 minutes. The changes that we made to the study design were minor and did not have a noticeable impact on the first two interviews which is why we decided to include the pilot interviews in the final data set.

4.2 Data Analysis

We transcribed the audio recordings at an orthographic level while preserving longer pauses and other non-verbal cues if deemed necessary. We did not translate interviews, as all researchers involved in the project are fluent in German. Afterward, we read the data multiple times to get a better understanding of our interviews. In order to analyze our data and provide answers to the research questions, we chose a two-fold approach, based on the thematic analysis approach as described by Braun and Clarke [8].

For RQ1, two researchers individually coded disjoint subsets of the interviews without prior discussion (open coding). Then, they merged their codebooks together, discussing codes, joining and splitting them as necessary. They also restructured the codebook and grouped related codes into categories. The resulting mind map and codebook, together with notes we took throughout the process, formed the basis for the thematic analysis. After the initial analysis, we agreed to construct types of verification behavior. One researcher constructed these types, which can be described as a specific form of theme, by iteratively going through the data, enhancing the types, and checking back if they still fit with previously seen data. We then discussed the resulting types, polishing them in the process.

For RQ2, one researcher performed open coding on an initial subset of five interviews. A second researcher used the resulting codebook to code the same transcripts. The Cohen's Kappa after this step was 0.72, which indicates a satisfactory agreement between the coders [34]. Both researchers met to discuss their results, especially mismatches in the coding. After resolving misunderstandings and adjusting for inaccuracies in the coding process, the value for Cohen's Kappa increased to 0.89, indicating an almost perfect agreement [34]. As a result of this discussion, we also adjusted the codebook by removing, adding and updating codes as necessary.

After this step, one researcher coded the remaining interviews, while only sparsely adding new codes when necessary. The same researcher then performed an axial coding step and started developing higher-level themes with the second researcher from initial ideas noted during the coding process. The first researcher continued this process of developing higher-level themes and wrote the report.

4.3 Recruitment and Participants

We recruited personnel from workplaces where it was mandatory to verify the EUDCC on a regular basis at some point during the pandemic. At the time of this study, this included most retail stores, restaurants, and other indoor venues such as theaters and cinemas. We recruited participants both locally (talking to people at their workplace, flyers) in Saarbrücken, Germany, as well as through an email campaign. Since legislation differs among German states, we only recruited par-

ticipants in the state of Saarland to ensure that all verifiers operated under the same legal framework.

In total, we recruited 17 participants (summarized in Table 1). We stopped recruiting after 14 participants and started analyzing our data, since we suspected to have reached saturation at this point. We later conducted three more interviews which confirmed our presumption. Due to the ongoing pandemic, we conducted most interviews (15/17) online. We interviewed the remaining two participants at our facility and their workplace, respectively. Each participant received a 15 Euro Amazon voucher as compensation.

We recruited twelve women and five men. Their average age was 32.9 ($\delta = 24.1$, median = 30). Five participants completed secondary school, seven completed high school, and five held a bachelor's or master's degree. We also questioned participants about their smartphone usage and their habit of interacting with an app to store the EUDCC. Seven participants reported using a smartphone frequently, eight reported regular usage and two disclosed very low usage. Ten participants reported using an EUDCC storage app frequently, with three reporting using one sometimes. The remaining four disclosed rarely using a storage app or not at all.

We managed to recruit participants holding a variety of jobs: five people worked in a theater or cinema, three had a job in a restaurant or bar, three worked in retail, two participants were gym employees, two front office workers at a large company, and one participant each was a hairdresser and paramedic respectively. In total, we interviewed people from 14 different workplaces.

Table 1: Participant demographics ($N = 17$).

Demographics	Participants (%)		
Gender			
Female	12	(70.6%)	
Male	5	(29.4%)	
Age			
18 - 28	7	(41.2%)	
29 - 39	5	(29.4%)	
40 - 50	3	(17.6%)	
51+	2	(11.8%)	
Highest Education			
Secondary School	5	(29.4%)	
High School	7	(41.2%)	
Bachelor's, Master's	5	(29.4%)	
Workplace			
Theater, Cinema	5	(29.4%)	
Retail	3	(17.6%)	
Restaurant, Bar	3	(17.6%)	
Front Office	2	(11.8%)	
Gym	2	(11.8%)	
Hairdresser	1	(5.9%)	
Paramedic	1	(5.9%)	

4.4 Ethical Considerations

This study has been reviewed and approved by our institution's ethical review board (ERB). The study design minimizes the collection of personally identifiable information as far as practical and all the collected data is stored and processed in line with GDPR. Every participant filled out a consent form and was given the opportunity to ask questions about the study before, during, and after the interview. We informed participants about their right of consent withdrawal or stopping the interview at any time including after the interview.

5 Results

In this section, we present answers to our research questions. We obtained these findings through a qualitative analysis of our data. We evaluated both the transcribed interviews and our observations of how participants verify certificates during the scenarios (see Section 4.1). First, we report the results relevant to *RQ1: How do professional users verify the EUDCC?*

These findings help us understand how the verification is regularly performed by professionals in real-world contexts giving us a more accurate picture of the distinct processes and subtle differences that occur in such a complex system outside of a controlled environment.

Throughout this section, we refer to participants as P1-17. We translated all direct quotes from German.

5.1 Verification Patterns

We analyzed our data as described in Section 4.2 to identify how users verify EUDCCs in a professional environment. We observed different behavioral building blocks which constitute our participants' verification approaches. We report the results obtained from the open and axial coding steps.

Scanning The dominant step in the verification process was scanning the certificate. Users would use a smartphone to scan a customer's QR code and rely on the result displayed by the verification app. While almost all participants used a designated verification app (e.g., CovPassCheck), one participant reported using the same app as for keeping their own certificate (see Section 2.2), hence storing all certificates permanently on their device. Most participants who regularly scanned certificates, stated to have received a suitable device from their workplace, others used their private smartphone.

> *"He can show me [the certificate] and then I scan it with my phone or with the phone from work. You have to do that. So I open my phone, I put it on the QR code, then I get a name and how old he is." - P3*

However, some participants in our study were not aware that the verification app is publicly available for all devices. They thought that only authorized entities had access.

> *"It's mainly for businesses. As an individual, you have this certificate, you have this [storage] app, and for the company there is another app [...] and unfortunately we don't have this app." - P9*

Participants reported that scanning occasionally fails due to wrinkled paper or reflections. Then they felt the need to revert to alternative methods.

Checking ID Verifying the claimed identity of the certificate holder was another important step in most participants' verification process. For the most part, it involved matching the face, name, and date of birth using the presented picture ID.

> *"I scan [the certificate] and get the name of the person in my app, can then compare it with the ID and thus verify the identity of this person." - P13*

While most participants used the data obtained by scanning the certificate, some gathered the relevant information directly from the presentation medium, i.e., the app in the first or the paper in the third scenario. A few users put in extra effort when checking the ID card, such as verifying that it was still valid.

Visual Verification Besides scanning the QR code, we found that participants were taking into account additional information visible to them when assessing a certificate. This information comes in different shapes. Verifiers would look for personal data present alongside the certificate, e.g., date of vaccination. This kind of information is included either in submenus of the app or on the paper version and is intended for the certificate holder, but not for verification purposes.

> *"You can obviously see [the information] when you scroll down, actually you should tap on it, and then there is all this information." - P1*

The same users might then self-assess the plausibility of the data, e.g., whether the date of vaccination is realistic for the perceived demographic of the customer. Our participants also considered visual cues of the presentation medium. These are features of the app's UI or design properties of the paper certificate, e.g., colors and fonts.

> *"The first thing that always catches the eye is that it is dark blue, which is always the case when the person is fully vaccinated." - P2*

Participants demonstrated to have specific expectations of what a certificate should look like. These were mostly based on what they are used to seeing (including their personal certificate), but partially also on what supervisors told them. Most participants were familiar with the certificates presented in scenarios one and three.

> *"I know what it looks like in my Corona app, my vaccination certificate, and I just make sure that it looks like mine, because mine is real." - P2*

Several participants explicitly checked whether the customer presented them with a picture of a certificate, e.g., a screenshot of an app. In scenarios one and two, they would interact with the device by trying to click or scroll through the contents.

Assessment of Certificate Holder The final building block was a person assessment of the certificate holder. Some participants assessed a customer's vaccination claim on the basis of trust. They would, in most cases, perform a visual verification, e.g., check if PII would match the appearance of the certificate holder, and then verify the validity based on the perceived trustworthiness of the person in front of them.

> *"[The woman in scenario two] looks very trustworthy. I don't expect her to download anything fake and show it to me." - P10*

Some participants demonstrated to be open to explanations from the presenter if a certificate would fail their initial verification. Again, these users would then perform an assessment of the person's credibility.

Furthermore, participants reported verifying less strictly if they anticipate negative consequences based on their assessment of the presenter. We distinguished between direct consequences, where verifiers felt intimidated by customers or feared immediate (physical) repercussions, and indirect consequences, i.e., entailing negative reactions from their supervisor or employer, such as losing their job after checking specific important customers.

> *"As a young woman, it once happened to me that a few guys came in and they all obviously had a screenshot. I worked alone so unfortunately I could do nothing but accept it." - P1*

Additionally, the medium the customer presents the certificate on also reflects on them. Some verifiers would get suspicious when customers presented the paper version, as we recreated in the third scenario. However, this only applies when they perceive the holder as tech-savvy enough to use a digital certificate.

> **Takeaways**
>
> We identified the main building blocks of verification behavior our participants employ when checking certificates. While most used the appropriate app, one participant employed the storage app for scanning. Some participants were not aware that official verification apps are publicly available. Checking IDs was straightforward, but some participants would match PII to data included alongside the QR code rather than the information obtained from scanning the certificate. In addition to the technically correct process, verifiers would check visual cues of the EUDCC and assess certificate holders' trustworthiness.

5.2 Verification Behavior

The behavioral patterns above constitute building blocks for different verifier classes. Based on a thematic analysis of our data, we developed four distinct types, which look as follows:

Type I: Consistent & Correct

This type of behavior judges the validity of a document solely on the result obtained from the verification app. It displays a consistent verification procedure (observed across all scenarios), which follows the correct process as detailed in Section 2.1. This approach can be best described as straightforward in that corresponding users will scan a person's certificate upon presentation without considering superfluous aspects such as, e.g., the app used to store the certificate or the appearance of the certificate holder. Users showing this type of verification behavior also never fail to cross-check the identity of the certificate holder with an official identity document. Based on our data, we theorize that this type is founded on a strong trust in the verification app and/or the EUDCC's underlying system.

Type II: Augmented Verification

Similar to Type I, this type is characterized by also scanning all certificates presented, but also involves examining additional information in the verification process. This additional information could stem from a visual verification of the certificate and its data. Users demonstrating this behavior will, for instance, get suspicious if the certificate deviates from their expectations. An assessment of the certificate holder could lead to suspicion in a similar way. However, these suspicions will not directly influence the verification process, i.e., users demonstrating this behavior will scan a certificate regardless of whether they are suspicious or not. While Type II behavior almost always includes cross-checking with an ID, we theorize that users showing this behavior, in comparison to Type I, have less trust in the app/the underlying system, or apply different threat models.

Type III: Selectively Scanning

Type III is characterized by an inconsistent verification process which involves scanning the certificate only occasionally. Users demonstrating this behavior will judge certificates primarily on the basis of a visual verification, while occasionally also relying on an assessment of the certificate holder. Similar to Type II, they will look at personal data and visual cues present alongside the QR code. If any details are outside of what users perceive as ordinary, this will raise suspicion and trigger scanning the certificate as an additional verification measure. We observed most suspicions when discussing the second scenario. The unfamiliar UI and lack of visual information made verifiers skeptical. Practicality was another potential justification for scanning only occasionally. Users perceived scanning a certificate as more time-consuming than a visual or trust-based verification.
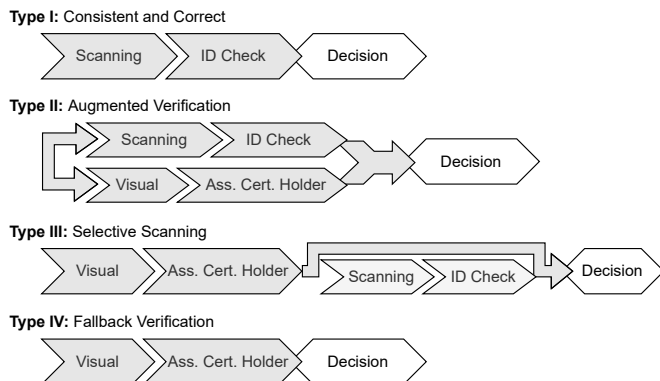
Type I: Consistent and Correct

Scanning → ID Check → Decision

Type II: Augmented Verification

Scanning → ID Check
Visual → Ass. Cert. Holder → Decision

Type III: Selective Scanning

Visual → Ass. Cert. Holder → Scanning → ID Check → Decision

Type IV: Fallback Verification

Visual → Ass. Cert. Holder → Decision

Figure 3: Verification behavior types based on behavioral patterns

Type IV: Fallback Verification

The fourth type distinguishes itself by generally not scanning certificates, even though corresponding verifiers are well aware of that option. However, from their point of view, they lack the necessary hard- or software to do so. While some might be under the impression that a specialized device is needed for scanning, others explicitly do not want to use their personal phone at work. Similarly, some verifiers are under the impression that only authorized entities, such as business owners, can access the required software.

In all Type IV cases, the employer did not provide a suitable device to their employees. In the absence of the possibility to scan the certificate, users fall back on employing visual verification as well as a trust-based assessment of the certificate holder to determine the validity. In cases where none of these strategies work, users would eventually reach out to a supervisor for assistance or resort to the WHO-style analog International Certificate of Vaccination or Prophylaxis (ICVP), if available. When discussing the second scenario, participants exhibiting Type IV behavior commonly argued that they could not determine the validity since it featured no information for visual verification.

> **Takeaways**
>
> We identified four types of verification behavior (see Figure 3), comprised of the building blocks described in Section 5.1. Type I performs a correct and secure verification. Type II carries out all necessary steps but also includes unnecessary visual and trust-based verification, indicating a distinct understanding and threat model. Type III occasionally performs a technically correct verification but will more often rely on gut feeling when assessing a vaccination claim. Finally, Type IV does not scan and incorrectly resorts to assessing the plausibility of available visual information. Table 2 presents our participants' observed resources, knowledge, and behavior, along with the type we assigned them.

5.3 Users' Understanding of Verification

In this section, we address *RQ2: What understanding do professional users have of the underlying verification process of the EUDCC?* We report the results of the thematic analysis we performed on the transcribed interviews. Our results suggest that users' perceived threat models with respect to the EUDCC verification procedure are a fundamental component of their underlying understanding.

5.3.1 Threat Models

We found that the threat models users have in the context of the EUDCC verification procedure are a crucial part of their understanding, as verifiers would often justify their behavior with perceived risks.

Screenshots The most commonly mentioned threat were screenshots. Some participants assumed screenshots to be invalid in every case hinting at an incorrect understanding of the technology or a very high level of caution. Other verifiers explained that they become suspicious when presented with a screenshot. However, they would not immediately assume invalidity or forgery as displayed by Type II behavior. Instead, their suspicion arises out of knowledge about possible image manipulation of screenshots resulting in a visually legitimate certificate as long as it is not scanned electronically. Out of these users, most doubt that any manipulation is possible inside the certificate storage app.

> *"[W]ith a screenshot, I cannot see that they are inside the app, and you can also change [the certificate]. When I scroll around in the CovPass app, the person cannot change anything, but with a screenshot you can just insert another QR code or something, I think[.]"* - P12

Other screenshot-suspicious participants knew that properly scanning the QR code could alleviate their distrust. Thus, they demonstrated their awareness of the certificate being securely contained within the QR code. They understand the limited reliability of the human-readable data accompanying the digital certificate.

Participants commonly mentioned presenting another person's certificate as a possible circumvention technique in connection with screenshots. Such certificates could be obtained from friends, family members, or even stolen. This is also a reason why screenshots constitute suspicion in some participants' understanding. However, most participants also mentioned that checking the ID mitigates this circumvention technique.

Malicious Signed Certificates Several participants voiced their concern about seemingly-correct signed certificates obtained by individuals who are not eligible for it (i.e., have not received the required vaccination). Their worries root in how the German system can be abused by presenting a forged

Table 2: Participant resources, knowledge, and behavior

Participant	Employer-provided Device[1]	Aware of Public Verification App[1]	Crypt. Signature Knowledge[2]	Knowledge Source(s)[3]	Used Verification App[1]	Behavior Type
P1	×	×	No Data	WO	×	IV
P2	✓	?	No Data	E, M	×	III
P3	✓	×	No Data	E	✓	I
P4	×	×	○○○	M	×[4]	III
P5	✓	✓	●●●	E, M	✓	I
P6	×	✓	○○○	E, ST	✓	II
P7	✓	×	●●○	E	✓	I
P8	✓	×	○○○	E	✓	I
P9	×	✓	○○○	E,C	×	IV
P10	×	?	○○○	C, ST	×	IV
P11	×	✓	●○○	M	×	IV
P12	✓	✓	○○○	E, C	✓	III
P13	✓	×	○○○	C	✓	II
P14	✓	×	●●○	E	✓	I
P15	×	✓	●○○	WO	✓	II
P16	×	×	○○○	ST	×	IV
P17	✓	✓	○○○	E, C	✓	II

[1] Symbols: ✓ Yes, × No, ? Unclear
[2] Knowledge: ○○○ None, ●○○ Weak, ●●○ Medium, ●●● Strong
[3] Knowledge Source(s): **WO** Watching Others, **E** Employer, **M** Media, **ST** Self-Taught, **C** Colleagues
[4] P4 incorrectly used the storage app to scan certificates.

paper-based ICVP, also known as a Yellow Card, at a pharmacy and get a EUDCC issued. Most users mentioning this threat also understood that they could not detect a maliciously signed EUDCC. Thus, they demonstrated awareness of the limitations of the verification they perform.

> *"Maybe someone has a [paper-based ICVP], goes to their general practitioner and tells them 'I lost my document, can you issue a new one' or at the pharmacy, I heard many did this: they created a counterfeit vaccination booklet, went to the pharmacy and still received that QR code."* - P6

5.3.2 Technical Understanding of the Verification Process

The understanding of the technical foundations of EUDCC is generally weak, with few exceptions. While a strong understanding was an indicator of a correct verification in our sample, the opposite is not true. A weak understanding did not mean that an individual would perform an incorrect verification.

Some participants who scanned the certificates with the appropriate app (exhibited by behavior Type I & II) expressed their trust in the tool to correctly verify the certificate without knowing how it actually works. In these cases, the trust in the technology motivated the correct behavior.

However, other participants who mostly performed the verification visually and considered this a proper technique (behavior Type III & IV) lacked the correct understanding of the technology and also did not consider an additional tool necessary. Based on their verification approach, they perceived screenshots as a threat, further emphasizing missing technical knowledge.

The paper and app-based variants of the EUDCC were perceived differently by many participants, both by those verifying visually as well as by those scanning the certificates. Most explained that they prefer to be presented with a certificate digitally as it is more secure than the paper-based variant.

> *"When you have [the EUDCC] in the app, it is hard to [forge] because you have to adjust it to your ID and that's why it's hard, for example, when you get [the EUDCC] from your father, then your date of birth and name won't be correct, that's why I think it's much more secure in the app. There it is hard to scan, I really don't know how that would work. But with a [paper] document it is obvious. Everyone knows Photoshop."* - P3

These participants assume different security guarantees between the two variants implying an incorrect perception of the EUDCC regarding the notion that all of the necessary information for the verification is stored inside the QR code.

A few users who demonstrated an understanding of the QR code's role in the technology also displayed less suspicion towards unknown UI elements, indicating that it is beneficial to have knowledge about some technical aspects of the EUDCC.

> *"I cannot imagine any [threats]. There is a [QR] code: it is valid or it is not."* - P7

With one exception, none of the participants showed a good understanding of digital signatures and what role they play in the verification process. Furthermore, users who relied mostly on visual verification had a particularly weak or no understanding of digital signatures.

5.3.3 User Education

The information sources on the verification procedure varied among participants. However, most did not learn the correct process solely from their employer, who was generally the person requesting them to perform the verifications. Instead, most participants learned their version of the verification procedure from elsewhere. Some reported looking it up on the Internet themselves or learning it through public media such as the news. Others mentioned that the process is easy and self-explanatory. Notably, some of these users did not perform the verification correctly.

"I informed myself on the Internet. It was some official website, some ministry page." - P11

During the interview phase, it became apparent that a very small number of users were unaware that certificate verification requires a separate app and they used a certificate storage app for scanning instead. By doing this, they unintentionally saved any scanned certificate persistently on their device, thus violating the privacy of the certificate holder.

Takeaways

Participants have a varying understanding of the verification process and technical aspects of the EUDCC. A central part of this understanding are the verifiers' threat models, of which screenshots are the most prominent, especially for verifiers performing a visual assessment. Even though the verifier cannot detect them, maliciously signed certificates were also commonly mentioned as threats. The majority of the participants showed a weak understanding of the technical foundations of the EU-DCC, but this was not an indicator of incorrect verification. Most participants did not solely learn the verification procedure from their employer but from other sources such as the media.

---

6   Discussion

Machine-readable visual certificates are here to stay. The economies of scale and ease of issuing make them cost-effective and quick to deploy. They can be presented on paper or smartphones, making them convenient for (tech-savvy) users, and are verifiable offline (i.e., no infrastructure dependence and better privacy). We can expect more future uses for such documents. Hence, it is crucial to understand how verifiers can be better supported in protecting the security and privacy of digital certificates and their owners.

6.1   Verifiers Misuse Auxiliary Data

Our findings show that verifiers often looked at visual cues presented alongside the QR code when assessing a certificate (see Section 5.1), e.g., a blue border around the QR code. Similarly, participants considered written information displayed in the certificate storage app, such as the vaccination date or the name.

Since the certificate holder is in complete control of their device, all information not included in the digital certificate, and therefore not cryptographically signed, must not be assumed authoritative. A motivated attacker could mimic a popular storage app and display arbitrary data. By relying on such cues and not checking the signature with an adequate tool, the verifiers void the security guarantees.

Previous work [15,16,40,47] has shown that users are often confused about the meaning of security indicators and wrongfully associate them with security guarantees, e.g., a web page being trustworthy if a green HTTPS indicator is present. Similar to what Dhamija et al. [15] and Bianchi et al. [7] found, some participants did not consider (or underestimated) how easily attackers can spoof a legitimate interface.

Therefore, we suggest removing visual cues and auxiliary data (including the holder's name) that are not relevant to the verification process. Thus, verifiers are not tempted to misuse them. Most additional information that current certificate storage apps provide is meant for the certificate holder, e.g., to check that the correct certificate was stored or to easily identify an expired one. We suggest separating these two use cases (i.e., verification vs. data inspection) into different areas of the applications. Each should have a dedicated interface, as opposed to one interface providing both features. The view presenting the certificate should not contain any visual cues, while the one for owners can make use of some indicators. In doing so, the app can also easily convey which information is needed for verification and which should be private to the certificate holder.

6.2   Verifiers Have Incomplete Threat Awareness

Most verifiers we interviewed demonstrated awareness of threats coming from the certificate presenters (see Section 5.3.1). Most commonly, these threats included presenters showing screenshots of others' certificates. Maliciously-signed certificates without the holder being vaccinated were also frequently mentioned. However, our participants rarely talked about the threats resulting from their own incorrect verification – hinting at an incomplete understanding of the threat landscape. This includes some participants infringing upon the customers' privacy by persistently storing certificates.

The fact that most participants lack understanding of the verification process opens the door for abuse. For example, suppose a presenter knows a certain verifier only glances at the main screen of a certificate without scanning the QR code. In that case, they may present a screenshot of someone else's certificate to enter a venue.

Camp [11] has shown that if security risks are not effectively communicated, the perceptions of such risks can be inadequate and lead to insecure behavior. In addition, Zollinger et al. [54] demonstrated that it is not only important for users to know the correct procedure but that they also need to be aware of the verification's purpose to perform it properly. Many of our participants knew about the requirement to scan certificates. The fact that many still did not perform a correct verification suggests that they did not fully understand the purpose of doing so or the threats coming from this practice. The possibility of shortcutting verification could also have impacted their behavior in this context (see Section 6.1).

To facilitate a far-reaching and complete awareness of the threats verifiers face, it is crucial for them to receive consistent and coherent education not only about the correct verification procedure but also about the threats they face, what can go wrong, and how to react in such instances. The UIs of the verification and storage apps would also benefit from conveying relevant threats in appropriate places to help verifiers retain this knowledge over time. This advice extends beyond the context of EUDCC verification to all similar systems utilizing visual digital certificates, where verifiers are not fully aware of the attack surface.

6.3 Structural Issues Lead to Inconsistent Verification

Our participants were subject to several structural inconsistencies, as illustrated in Table 2: nearly half were not aware of the official, publicly available verification apps, only some employers provided a dedicated verification device, and their knowledge of correct certificate verification came from several (unofficial) sources. All these factors led to inconsistent, often insecure verification behavior. Sometimes, verifiers could not do their job properly due to fear of negative repercussions by either the customers or their employers. We also identified a potential conflict of interest: business owners and personnel could be incentivized to let customers in to increase their sales and tips, respectively. Hence, they might be inclined to perform less rigorous checks.

Such issues cannot be solved by looking at the purely *technical* side. EU legislation made it necessary to develop the EUDCC in a short time frame due to the immediate need for privacy-preserving electronic vaccination proofs. The rushed deployment, which focused on the technical aspects, underestimated the structural (legal) framework necessary for large-scale deployment. Business owners, who often have little knowledge about technical systems, were burdened with implementing vaccination-based access restrictions. These circumstances led to our participants' varying resources, knowledge, and behaviors, leaving them confused and unsure about key elements of the verification process, e.g., the proper response when detecting fake certificates.

We recommend that future systems come with actionable guidelines that cover coherent verifier education and are backed by a legal requirement for compliance. Employers must provide verifiers with an appropriate verification device and software. Doing so can also help mitigate the privacy threat of verifiers persistently storing certificates. Furthermore, it is necessary to create awareness of real-life conditions such as non-compliant certificate holders trying to skirt legal restrictions. Verifiers must have clear legislation-backed guidelines on how to behave in such cases, e.g., contacting the employer or authorities. As for the conflict of interest for the personnel, splitting the verifier and service role could aid in disarming it.

6.4 Transferring Our Insights to Other Contexts and Future Research

EUDCC was not the first European system to use digitally-secured paper passes but is arguably the biggest one. Due to many rail companies operating cross-country trips in Europe, often with personnel changing at borders, rail companies introduced digitally signed tickets a decade ago [21]. Visual digital certificates are also discussed for digital driver's licenses [52] or digitally signed drug prescriptions [25], among others.

Depending on the context, some requirements for visual digital certificates can be accomplished more easily than others: police officers, for instance, can be centrally trained to verify driver's licenses, which is more difficult to accomplish for employees of independent pharmacies when it comes to prescriptions. Similarly, depending on the typical work environment, verification devices can be installed on-site (e.g., at the entrance of a concert venue) or need to be mobile (e.g., in trains), which might require providing a device to each individual verifier. Issues surrounding missing knowledge about threat models are likely to persist across contexts where verifiers are commonly less tech-savvy. This can be especially relevant when deploying digital certificates to replace an established system. Many analog documents rely on visual cues to assert authenticity, such as holograms on driver's licenses [46]. Therefore, extra effort is necessary, both from a design perspective as well as training, to adapt verifiers' behavior to the new security features.

Finally, a decisive factor to consider is the verifiers' motivation. As mentioned above, in the COVID setting, we saw a potential conflict of interest. This does not necessarily hold in other contexts, e.g., train companies inspecting passengers' tickets, where a sub-par verification would lead to a decrease in revenue.

For future work, we suggest investigating visual digital certificates in contexts beyond COVID certificates and expanding on verification behavior in a broader way. Furthermore, QR codes are an interesting topic when used in such circumstances, as they are often still wrongly associated primarily with marketing (e.g., on billboards) or games. Past research mostly focused on those aspects as well as partially on security and privacy aspects [13, 14, 33, 35]. Future work should expand on users' understanding of QR codes as carriers for digital certificates and other security-related applications.

6.5 Limitations

Previous work [41] has shown that privacy awareness can impact people's privacy behavior. Thus, verifiers' awareness of potential privacy infringements might influence their behavior. However, we did not collect data on participants' attitudes towards vaccine mandates or a general aversion to state-mandated regulations. More detailed information on

work experience with digital certificate verification could provide further insights. To keep the study simple and to avoid fatigue, we only asked for an estimate of verification procedures per work day and how long they had been verifying certificates.

We carefully chose three scenarios to cover the most common real-world situations from the participant's point of view while also investigating their understanding of the technology. However, more real-world situations remain for future work to investigate. Furthermore, while some observations are specific to certain scenarios, others are consistent across scenarios, as indicated in the results. The scenario ordering and legislation at the time of the study may have introduced further limitations. Due to the pandemic, we conducted an online lab study, which can introduce biases (e.g., response bias) compared to real-world observations.

7   Conclusion

Visual digital certificates are becoming increasingly common and are considered the future technology for digital driving licenses. However, the effectiveness of such visual digital certificates heavily relies on correct handling by the enforcing personnel.

We explored how professionals in various industries verify the QR-code-based EUDCC as part of their job. We examined and tested their understanding of the security features and their verification.

We identified and classified varying behavior patterns, including inadequate reliance on visual cues as a proxy for proper digital verification. These patterns and our findings on verifiers' benefit and threat perceptions of visual digital certificates allow us to understand user behavior and provide directions for exploring the design space. Our empirical results and discussion of future research directions with a strong focus on user perspectives are essential for improving the robustness of visual digital certificates and helping ensure theoretical security benefits in practice.

References

[1] Corona-Warn-App - GitHub - Release v2.11.0-RC1. https://github.com/corona-warn-app/cwa-app-ios/releases/tag/v2.11.0-RC1, 2021. [Accessed: 2022-10-04].

[2] Digitaler-Impfnachweis - GitHub - Release v1.11.0. https://github.com/Digitaler-Impfnachweis/covpass-ios/releases/tag/v1.11.0, 2021. [Accessed: 2022-10-04].

[3] Digitaler-Impfnachweis - GitHub - Release v1.15.0. https://github.com/Digitaler-Impfnachweis/covpass-ios/releases/tag/v.1.15.0, 2022. [Accessed: 2022-10-04].

[4] Digitaler-Impfnachweis - GitHub - Release v1.17.0. https://github.com/Digitaler-Impfnachweis/covpass-ios/releases/tag/v1.17.0, 2022. [Accessed: 2022-10-04].

[5] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS)*, 2019.

[6] Ruba Abu-Salma, Elissa M Redmiles, Blase Ur, and Miranda Wei. Exploring user mental models of end-to-end encrypted communication tools. In *8th USENIX Workshop on Free and Open Communications on the Internet (FOCI)*, 2018.

[7] Antonio Bianchi, Jacopo Corbetta, Luca Invernizzi, Yanick Fratantonio, Christopher Kruegel, and Giovanni Vigna. What the App is That? Deception and Countermeasures in the Android User Interface. In *2015 IEEE Symposium on Security and Privacy*, 2015.

[8] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[9] Bundesminister für Soziales, Gesundheit, Pflege und Konsumentenschut. 3. COVID-19-Maßnahmenverordnung – 3. COVID-19-MV. *Bundesgesetzblatt für die Republik Österreich*, (441. Verordnung), 2021. Available: https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2021_II_441/BGBLA_2021_II_441.pdfsig [Accessed: 2022-10-04].

[10] Bundesregierung. Beschluss - Top 2: Maßnahmen zur Bewältigung der Corona-Pandemie. *Videoschaltkonferenz der Bundeskanzlerin mit den Regierungschefinnen und Regierungschefs der Länder am 10. August 2021*, pages 3–7, 2021. Available: https://www.bundesregierung.de/resource/blob/974430/1949532/

d3f1da493b643492b6313e8e6ac64966/2021-08-10-mpk-data.pdf [Accessed: 2022-10-04].

[11] L. Jean Camp. Mental models of privacy and security. *IEEE Technology and Society Magazine*, 28(3):pages 37 – 46, 2009.

[12] European Commission. EU Digital COVID Certificate. https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en, 2021. [Accessed: 2022-10-04].

[13] Adrian Dabrowski, Isao Echizen, and Edgar R. Weippl. Error-correcting codes as source for decoding ambiguity. In *Proceedings of Workshops at IEEE Security & Privacy*, 2015.

[14] Adrian Dabrowski, Katharina Krombholz, Johanna Ullrich, and Edgar Weippl. QR inception: Barcode-in-barcode attacks. In *Proceedings of the 4th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, 2014.

[15] Rachna Dhamija, J. D. Tygar, and Marti Hearst. Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI, 2006.

[16] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. You've been warned: An empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI, 2008.

[17] eHealth Network. Guidelines on Technical Specifications for EU Digital COVID Certificates Volume 2. *EU Digital COVID Certificate Gateway*, (Version 1.5), 2022. Available: https://health.ec.europa.eu/system/files/2022-07/digital-covid-certificates_v2_en.pdf [Accessed: 2022-10-04].

[18] eHealth Network. Guidelines on Technical Specifications for EU Digital COVID Certificates Volume 4. *EU Digital COVID Certificate Applications*, (Version 1.5), 2022. Available: https://health.ec.europa.eu/system/files/2022-07/digital-covid-certificates_v4_en.pdf [Accessed: 2022-10-04].

[19] Marc Eisenstadt, Manoharan Ramachandran, Niaz Chowdhury, Allan Third, and John Domingue. COVID-19 Antibody Test/Vaccination Certification: There's an App for That. In *IEEE Open Journal of Engineering in Medicine and Biology*, volume 1, pages 148–155, 2020.

[20] European Union. Commission Delegated Regulation (EU) 2021/2288 of 21 December 2021 amending the Annex to Regulation (EU) 2021/953 of the European Parliament and of the Council as regards the acceptance period of vaccination certificates issued in the EU Digital COVID Certificate format indicating the completion of the primary vaccination series. *OJ*, L 458. Available: http://data.europa.eu/eli/reg_del/2021/2288/oj [Accessed: 2022-10-04].

[21] European Union Agency for Railways. Digital security elements for rail passenger ticketing. *Technical document, TAP TSI TD B.12, ERA-REC-122/TD/02*, (Version 2.0), 2022. Available: https://www.era.europa.eu/sites/default/files/library/docs/recommendation/era_rec122_tap_tsi_revision_recommendation_technical_document_b12_en.pdf [Accessed: 2022-10-04].

[22] Federal Ministry of Health. How the digital vaccination certificate works. https://www.zusammengegencorona.de/en/how-the-digital-vaccination-certificate-works/, 2022. [Accessed: 2022-10-04].

[23] Federal Statistical Office. Current population of germany. 2022. Available: https://www.destatis.de/EN/Themes/Society-Environment/Population/Current-Population/_node.html [Accessed: 2022-10-04].

[24] Kevin Gallagher, Sameer Patil, and Nasir Memon. New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[25] gematik. E-Rezept. https://www.gematik.de/anwendungen/e-rezept. [Accessed: 2022-10-04].

[26] Josh Groeneveld. In Deutschland gilt in Restaurants und Bars die 3G-Corona-Regel. Doch eine Umfrage zeigt, wie selten sie kontrolliert wird. *Business Insider*, 2021. Available: https://www.businessinsider.de/politik/deutschland/in-deutschland-gilt-in-restaurants-und-bars-die-3g-corona-regel-doch-eine-umfrage-zeigt-wie-selten-sie-kontrolliert-wird-a [Accessed: 2022-10-04].

[27] Maximilian Häring, Eva Gerlitz, Christian Tiefenau, Matthew Smith, Dominik Wermke, Sascha Fahl, and Yasemin Acar. Never ever or no matter what: Investigating Adoption Intentions and Misconceptions about the Corona-Warn-App in Germany. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS)*, 2021.

[28] Albert B. Jeng and Lo-Yi Chen. How to enhance the security of e-Passport. In *2009 International Conference on Machine Learning and Cybernetics*, volume 5, pages 2922–2926, 2009.

[29] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. "My Data Just Goes Everywhere:" User

Mental Models of the Internet and Implications for Privacy and Security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS)*, 2015.

[30] Georgios Karopoulos, Jose L. Hernandez-Ramos, Vasileios Kouliaridis, and Georgios Kambourakis. A Survey on Digital Certificates Approaches for the COVID-19 Pandemic. In *IEEE Access*, volume 9, pages 138003–138025, 2021.

[31] Marvin Kowalewski, Franziska Herbert, Theodor Schnitzler, and Markus Dürmuth. Proof-of-Vax: Studying User Preferences and Perception of Covid Vaccination Certificates. In *Proceedings on Privacy Enhancing Technologies*, volume 1, pages 317–338, 2022.

[32] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. "If HTTPS Were Secure, I Wouldn't Need 2FA" - End User and Administrator Mental Models of HTTPS. In *IEEE Symposium on Security and Privacy*, 2019.

[33] Katharina Krombholz, Peter Frühwirt, Peter Kieseberg, Ioannis Kapsalis, Markus Huber, and Edgar Weippl. QR Code Security: A Survey of Attacks and Challenges for Usable Security. In *Human Aspects of Information Security, Privacy, and Trust*, volume 8533 of *Lecture Notes in Computer Science*, pages 79–90. Springer International Publishing, 2014.

[34] J Richard Landis and Gary G Koch. The measurement of observer agreement for categorical data. *Biometrics*, 33(1):159–174, 1977.

[35] Shimon Machida, Adrian Dabrowski, Edgar Weippl, and Isao Echizen. Privacytag: A community-based method for protecting privacy of photographed subjects in online social networks. In Arpan Kumar Kar, P. Vigneswara Ilavarasan, M.P. Gupta, Yogesh K. Dwivedi, Matti Mäntymäki, Marijn Janssen, Antonis Simintiras, and Salah Al-Sharhan, editors, *Digital Nations – Smart Cities, Innovation, and Sustainability*, 2017.

[36] Karola Marky, Kirill Ragozin, George Chernyshov, Andrii Matviienko, Martin Schmitz, Max Mühlhäuser, Chloe Eghtebas, and Kai Kunze. "Nah, it's just annoying!" A Deep Dive into User Perceptions of Two-Factor Authentication. *ACM Transactions on Computer-Human Interaction*, 2021.

[37] Salima S. Mithani, A. Brianne Bota, David T. Zhu, and Kumanan Wilson. A scoping review of global vaccine certificate solutions for COVID-19. *Human Vaccines & Immunotherapeutics*, 18(1):1–12, 2022.

[38] Leysan Nurgalieva, Seamus Ryan, Andreas Balaskas, Janne Lindqvist, and Gavin Doherty. Public views on digital covid-19 certificates: A mixed methods user study. In *ACM Conference on Human Factors in Computing Systems*, CHI, 2022.

[39] Alexander Ponticello, Matthias Fassl, and Katharina Krombholz. Exploring Authentication for Security-Sensitive Tasks on Smart Home Voice Assistants. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS)*, 2021.

[40] Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo. Rethinking Connection Security Indicators. In *Twelfth Symposium on Usable Privacy and Security (SOUPS)*, 2016.

[41] Stefanie Pötzsch. Privacy Awareness: A Means to Solve the Privacy Paradox? In *The Future of Identity in the Information Society*, IFIP Advances in Information and Communication Technology, 2009.

[42] Robert Koch-Institut. Corona-Warn-App. `https://www.coronawarn.app/en`, 2021. [Accessed: 2022-10-04].

[43] Robert Koch-Institut. CovPass - Google Play. `https://play.google.com/store/apps/details?id=de.rki.covpass.app`, 2021. [Accessed: 2022-10-04].

[44] Robert Koch-Institut. CovPass-App. `https://www.digitaler-impfnachweis-app.de/en`, 2021. [Accessed: 2022-10-04].

[45] Robert Koch-Institut. CovPassCheck-App. `https://digitaler-impfnachweis-app.de/en/covpasscheck-app`, 2021. [Accessed: 2022-10-04].

[46] Pradeepa Samarasinghe, L.K.P Lakmal, A. V. Weilkala, W.A.N.P.C Wickramarachchi, and E.R.S. Niroshana. Sri lanka driving license forgery detection. In *2017 Fourth International Conference on Image Information Processing (ICIIP)*, 2017.

[47] Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. The Emperor's New Security Indicators. In *2007 IEEE Symposium on Security and Privacy*, 2007.

[48] Eric Spero and Robert Biddle. Out of Sight, Out of Mind: UI Design and the Inhibition of Mental Models of Security. In *New Security Paradigms Workshop (NSPW)*, 2020.

[49] Sophia Spyropoulos. Warum wird bei der Überprüfung von 3G/2G nicht der Ausweis kontrolliert? *MDR AKTUELL*, 2021. Available: `https://www.mdr.de/nachrichten/sachsen/drei-zwei-g-kontrolle-ausweis-100.html` [Accessed: 2022-10-04].

[50] Milica Stojmenović, Temitayo Oyelowo, Alisa Tkaczyk, and Robert Biddle. Building Website Certificate Mental Models. In Jaap Ham, Evangelos Karapanos, Plinio P. Morita, and Catherine M. Burns, editors, *Persuasive*

Technology, volume 10809 of *Lecture Notes in Computer Science*, pages 242–254. Springer International Publishing, 2018.

[51] Frida Thurm. 2G und 3G: Werden Corona-Regeln in Kneipen wirklich kaum kontrolliert? *Die Zeit*, 2021. Available: https://www.zeit.de/gesellschaft/zeitgeschehen/2021-11/2g-3g-corona-regeln-gastronomie-impfung-bars-restaurants-kontrolle [Accessed: 2022-10-04].

[52] Chris Velazco. Digital driver's licenses take the sting out of forgetting your wallet. Here's how they work. *Washington Post*, 2021. Available: https://www.washingtonpost.com/technology/2021/10/11/digital-drivers-license-mdl/ [Accessed: 2022-10-04].

[53] World Health Oranization. Novel Coronavirus(2019-nCoV) Situation Report - 10. 2020. Available: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200130-sitrep-10-ncov.pdf [Accessed: 2022-10-04].

[54] Marie-Laure Zollinger, Verena Distler, Peter B. Roenne, Peter Y. A. Ryan, Carine Lallemand, and Vincent Koenig. User Experience Design for E-Voting: How mental models align with security mechanisms. In *Proceedings of the International Joint Conference on Electronic Voting*. TalTech, 2021.

A   Interview Guideline

This is the English translation of the interview guideline. Actions taken by the interviewer are denoted in italic.

Introduction

Greet participant, introduce interviewer and topic: "Hello, thank you for participating in this interview about the verification of the EUDCC"
Hand out consent sheet, explaining purpose of study and how data is going to be used. After the consent sheet has been read and signed, commence with the interview and start the audio recording. "We are going to start with the interview now if you have no questions at the moment."
Wait for and answer questions. "First of all, I want to ask you some quick questions about your job so I can put your later answers in context better."

- What is your job title?

- How long have you been working this job?

- How often do you usually check Digital COVID Certificates during one working day?

Verification Task

Transition to Verification task: "Thanks for your answers so far. Now we will start with a task where I will present you with a few scenarios which include a person that comes to you with their COVID certificate and all you have to do is verify them as you would do in your everyday life at work. Since we have to do this online I would like to ask you to view these scenarios as if they were happening in the real-world. Please keep in mind that this is no test and I simply want to learn how you would usually do this. There are no rules or restrictions on how you can go about this. I just want to know if the certificates are valid and how you came to that conclusion so thinking out loud and explaining your reasoning as detailed as possible is very welcome. Also, if you have any questions you can ask me at any time."

For each scenario   *Present prepared scenario which includes a picture of a person with their name and date of birth and an accompanying certificate. Present only the certificate to the participant so they can interact with it freely. If the participant asks for some ID, show them the prepared ID for the respective scenario. Let participant verify, take notes about observations and ask follow-up questions if necessary.*

After Verification Task

"Thank you. This was all the certificates to verify. Now, I want to ask you a few questions about your understanding of the verification process of these certificates."

- Please walk me through the correct verification process as you understand it in as much detail as possible.

- How, if at all, has the verification process been explained to you?

  - **If it was explained:** Who explained the verification process to you?

  - **If it was not explained:** How did you learn about the verification process then?

- Are you aware of any ways to trick the verification process?

  - **If yes:** What are they and how can they be avoided?

  - **If no:** What about the design of the certificate makes it so hard to trick?

- Do you know what digital signatures are and how they work?

  - **If yes:** Can you please explain how they work?

B   Codebooks

The following tables contain the final codes we agreed upon during the data analysis. As described in Section 4, we used two distinct approaches, each including its own codebook.

Codebook I: Verification Behavior

Scanning the certificate
    Scanning without considering other factors
    Scanning even if suspicious
    Scanning only when suspicious
Visual Verification
    Verification based on PII
        User self-checks plausibility of data on certificate
        Missing PII leads to rejection of certificate
        Missing PII creates suspicion
    Checking visual cues
    Manually check vaccination count
Assessment of certificate holder
    Trust in presenter
    Fear of negative consequences
    Open to explanations while doubtful
Fallback strategies
    Fallback to visual verification if scanning fails
    Fallback to vaccination booklet if visual verification fails
    Fallback to contacting superior if verification fails
Explicitly not scanning
    Missing scanning device
    Not scanning for practicality reasons
Checking for screenshots
    Screenshot leads to rejection of certificate
    Screenshot creates suspicion
Cross-check with ID

Codebook II: Verifiers' Perceptions of Visual Digital Certificates

---

Threats
    Screenshot seen as threat
    Using another person's certificate as threat
    Vaccination booklet as threat
    Fake signed certificate as threat
    Physically stolen certificate as threat
    Phishing type attack as threat
Understanding
    Scanning required
    ID check required
    Verification process not explained at work
    Verification process learned in real world
    Verification process is self-explanatory
    Interaction with certificate required
    Certificate must contain PII visually
    Certificate must follow specific visual appearance
    Scanning requires special hardware/software
    Screenshot not valid
    Does know digital signatures well
    Does know digital signatures partially
    Does not know digital signatures
    Correct verification is secure
    Trust in the technology
    Mistrust in the technology
    Fake certificate obvious
Process
   Fallback to visual verification if scanning fails
    Vaccination booklet as fallback
    Visual cues used for verification
    User self-checks plausibility of data on certificate
    Saves certificate persistently
    Open to explanations while doubtful
    Manual verification of personal data
    Manually check vaccination count
Mentions familiarity of interface
Mentions unfamiliar interface
Prefers analogue certificate
Prefers digital certificate
Mentions privacy concerns

C Scenarios

The scenarios shown here were used for the verification task of the interview and contain valid COVID certificates that were kindly provided by friends and family members. Since these certificates belong to real people, we include blurred versions of the certificates used during the interviews.

When a participant asked for an ID during the verification task, we provided them with a fabricated ID that only contained the real name and date of birth belonging to the respective certificate. The other information on the fabricated IDs was made up. We provided no back side to the IDs as they would contain no information relevant to the task.
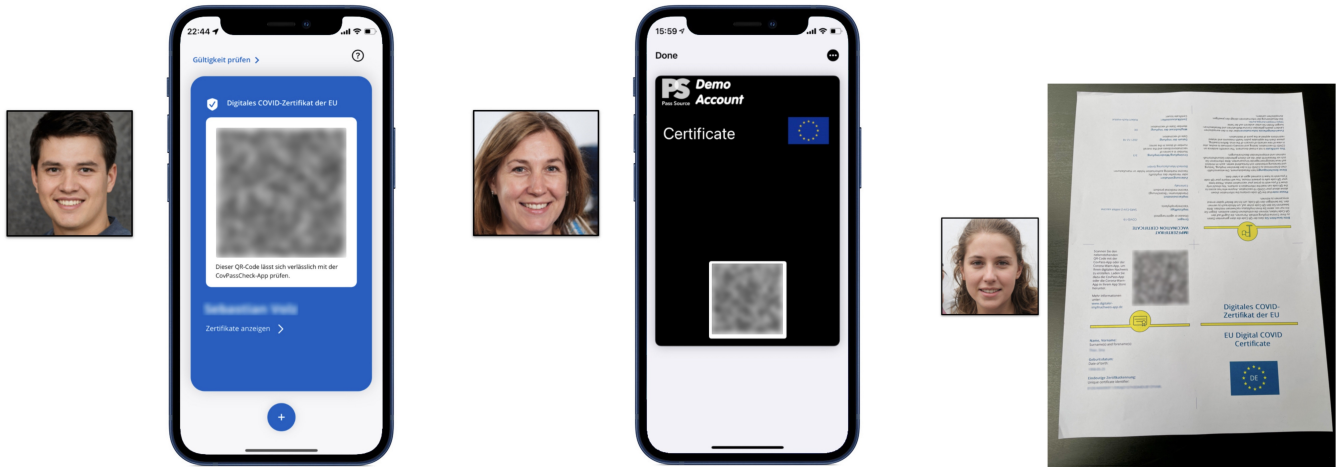
(a) Scenario 1: CovPass

(b) Scenario 2: Obscure UI

(c) Scenario 3: Paper

(d) Fabricated ID for Scenario 2

Figure 4: An example of a fabricated ID and the three scenarios