Tangible 2FA – An In-the-Wild Investigation of User-Defined Tangibles for Two-Factor Authentication

Mark Turner[1], Martin Schmitz[2], Morgan Masichi Bierey[1], Mohamed Khamis[1], Karola Marky[1,3]
[1]*University of Glasgow, United Kingdom,* [2]*Saarland University Saarbrücken, Germany,*
[3]*Ruhr-University Bochum, Germany*

Abstract

Although two-factor authentication (2FA) mechanisms can be usable, they poorly integrate into users' daily routines, especially during mobile use. Using tangibles for 2FA is a promising alternative that beneficially combines customisable authentication routines and object geometries, personalisable to each user. Yet, it remains unclear how they integrate into daily routines. In this paper, we first let 226 participants design 2FA tangibles to understand user preferences. Second, we prototyped the most common shapes and performed a one-week long in-the-wild study (N=15) to investigate how 2FA tangibles perform in different environments. We show that most users prefer objects that a) fit in wallets, b) connect to daily items or c) are standalone. Users enjoyed interacting with 2FA tangibles and considered them a viable and more secure alternative. Yet, they voiced concerns on portability. We conclude by an outlook for a real world implementation and distribution of 2FA tangibles addressing user concerns.

1 Introduction

Two-factor authentication (2FA) is has become part of our daily lives, with many services, from banks to major internet players offering the security benefits of 2FA [4, 7]. While these security benefits are undisputed and the early usability problems of the authentication procedure have been mainly resolved by constant improvements (cf. [9, 10]), newer research has shown that a large share of users are still reluctant to use 2FA beyond being forced to do so by their providers [1, 16, 17].

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, Anaheim, CA, USA

The reasons for that lie beyond usability in the users' daily lives, routines, and habits that are interrupted by current 2FA procedures, creating too much so-called *friction* [17, 20], for instance, by taking too long [6, 11, 32] or being not readily available [6, 16, 17]. While previous work has identified these general issues, finding appropriate alternatives that better integrate into users' daily routines and contexts remains an open research challenge.

Among possible alternatives are *tangible* interactions that better integrate into users' individual environments and routines by utilising digital fabrication [21]. Tangibles are physical objects used to manipulate digital information [25]. In the context of 2FA, tangibles can serve as personal user tokens. They either are the authentication factor ownership or form a complete 2FA mechanism. In 2020, 3D-Auth [18] was proposed as a tangible 2FA mechanism. It is based on using 3D-printed tangibles for 2FA that can be customised in terms of colour, and shape interaction and be integrated into other daily items, such as accessories. The 2FA tangible itself embeds a unique conductive structure that can be sensed by touchscreens and encodes the authentication factor ownership. By interacting with the 2FA tangible, users enter a kind of haptic password, e.g., by rotating parts of the tangible. This interaction represents the knowledge authentication factor. Consequently, 3D-Auth offers 2FA in one interface.

The knowledge-based interaction has been demonstrated to have a high memorability since it also leverages muscle memory [18]. What remains unclear though, is what kinds of 2FA tangibles users might want to use for authentication and how these tangibles perform when used on a daily basis. This paper contributes to the space of tangibles for 2FA by investigating the following research questions:

RQ1: *What kinds of 2FA tangibles do users wish to use?* We investigate what kinds of tangibles users wish to use in their daily routines and how they wish to interact with them. For this, we conducted an online study where we let 226 users configure their ideal tangibles.

RQ2: *How do tangibles for 2FA perform in the user's daily lives? What are the obstacles and challenges introduced*

by them? We investigate how 2FA tangibles as a 2FA mechanism that combines ownership and knowledge perform when used daily. For this, we first chose the top three 2FA tangible designs and developed them as prototypes. Second, we conducted an in-the-wild study (N=15) during which participants used the prototypes in their daily life over a whole week. Using short questionnaires during the interaction phase and in-depth interviews, we report and discuss positive aspects and emerging challenges for 2FA tangibles.

Research Contribution. In summary, the main contributions of this paper are:

User-Defined Tangibles: We investigate what kinds of tangible 2FA items users choose in an online study with 226 participants. We show what kinds of interactions users would like to perform for authentication and which shapes, sizes, colours, and further properties they prefer. Participants preferred rather simple geometric shapes, such as cubes or squares with sizes between one and ten centimetres to fit the smartphone screen.
In-the-Wild Investigation: Based on the results of the online study, we designed three tangible prototypes that realise a 2FA mechanism that combines the ownership and knowledge authentication factors. We used these tangibles in an in-the-wild study where 15 participants used the designed tangibles in their lives for a week. Our participants perceived the tangibles as adding a layer of security to their important accounts. In addition, the interactions were mostly perceived as easy-to-use and fun.
User-Centred Design Pipeline: We conclude by proposing a user-centred design pipeline that assists the users in designing 2FA tangibles specifically for their preferred usage environment, security needs, and user preferences. The design pipeline is not limited to standalone 3D-printed tangibles but also considers alternatives with integrated sensors to enable authentication for all kinds of devices, e.g., by using USB connections or NFCs.

2 Background and Related Work

In this section, we present background and related work that our research builds upon.

2FA Realisations. Several realisations of 2FA have been brought to the market or were proposed by related work. The usage of one-time passwords (OTPs), e.g., via text messages, emails, phone calls, or apps nowadays is well-established and used by a plethora of providers. Most of them require a smartphone to somehow access the OTPs. Another smartphone-based option without OTPs are push notifications where users press a button. For those who do not wish to rely on smartphones, OTP generators (e.g., DUO Security Token [29], or Fido U2F [8]) are an alternative. Based on security considerations, the second authentication factor should ideally be on a different device than the main interaction. For instance, if the authentication is done on a laptop, a smartphone or token can be used. If authentication is done on a smartphone, a token or another smartphone would be required. Investigations of real-world usage showed that users frequently use one device for authentication and main interaction [17] which defeats some security benefits of 2FA. Related work also showed that mobile users might not be willing to carry a dedicated OTP generator [17, 31]. Reasons for that were limitations in personalisation [17].

3D-Auth Concept [18]. In this paper, we use the concept 3D-Auth [18] as a basis for our investigation. The concept combines the security benefits of a separate token while also mitigating personalisation issues by allowing users to either choose a custom 3D-printed shape or integrate the token into an everyday object, such as an accessory.
Fabrication: 3D-Auth items are fabricated as follows: they have an internal authentication structure by embedding a capacitive material within insulating plastic. The capacitive material can be detected using a capacitive touchscreen. For this, each 3D-Auth item has a grid of conductive dots at the item's bottom. The conductive dots themselves are not sufficient for detection by the touchscreen, because users have to actively touch the item.
Interaction: Marky et al. [18] present five possible interaction categories for the knowledge-based part. First, users *touch* the item surface on specific spots or perform gestures. Second, users *arrange* one or multiple items on the touchscreen. Third, users *configure* the item by pressing or rotating parts of it. Fourth, users *assemble* a set of multiple items into one item. Finally, users change the item's internal configuration by *augmenting* it with something else (e.g., water or air).
2FA by 3D-Auth: 3D-Auth realises 2FA by splitting the conductive structure into two components: (1) a *static* component that encodes the authentication factor *ownership*. This makes up one subset of the conductive dots that are always sensible by the touchscreen and can be compared to a conductive token; and (2) a *dynamic* component that encodes the authentication factor *knowledge*. Through interaction, the dynamic part of the capacitive authentication structure is transformed in such a way that the change can be detected. This makes up another subset of the conductive dots that are turned into sensible touchpoints by user interaction. This interaction can be compared to a haptic password. Both structures together form the authentication pattern that is sensed by a touchscreen. It is a subset of the conductive dots in the object's bottom.
Security Aspects: 3D-Auth items protect accounts by proving two authentication factors in one item. In comparison to existing standalone authentication tokens that only encode the ownership factor (e.g., non-bio YubiKeys [35]), 3D-Auth offers a higher level of security because the item alone is not enough to impersonate the user due to the dynamic

authentication component. Further, the item cannot easily be replicated (e.g., by observation), because either the 3D printing file is needed, or the item has to be cut into several layers to reveal its entire internal structure. Assuming that an attacker takes over a device (e.g., a smartphone), 3D-Auth offer a higher level of security compared to OTPs via SMS, authenticator apps or other kinds of notifications, because the 3D-Auth item is physically separate from the device. Since this paper focuses on the human perspective of 2FA tangibles, we refer to the original 3D-Auth publication for more in-depth security-related information [18].

Tangible Authentication. Using tangible items for authentication has been proposed before in the scope of single-factor authentication, by using conductive sheets that cover parts of a touchscreen [30, 34] or a Rubik's Cube-like structure where interactions are captured with a camera [22].

Adoption and Usability of 2FA. The reasons for (not) adopting 2FA vary. The main criterion for using 2FA is the security benefit for protecting valuable assets [23, 24]. For instance, the amount of money in accounts impacts 2FA adoption; the more money, the more likely users protect the account with 2FA [23]. Further impacting factors are usability [3, 11, 32], trustworthiness [11], the required cognitive effort [11, 17] and familiarity with 2FA [6, 12, 33]. Abbott and Patil conducted a series of online surveys in a university where 2FA is mandatory [1]. They could not find the mandatory nature to impact the acceptance of 2FA. Instead, motivating users with personalised messages to assist them in adjusting their mental model of 2FA is promising to boost adoption [15].

The usability of different 2FA realisations has been thoroughly researched in the past. Yet, there is no overall consensus since the specific approach and its realisation seem to have a profound impact on usability. Further, two distinct usage phases have to be considered separately: 1) setup phase and 2) authentication phase [2, 26] that we discuss in the following.

The YubiKey [35] is a token that supports several cryptographic protocols, e.g., OpenPGP. It can be connected to a computer via USB or a smartphone via USB-C or NFC and is a possible second factor for 2FA. Participants in several user studies struggled to set up the YubiKey [2, 9, 24, 26]. This was also demonstrated for other tokens [5, 6, 32]. In contrast to tokens, the setup of OTPs by text messages [2, 5, 24], pre-generated OTPs [24], and push notifications [2, 24] was perceived as easier-to-use. Consequently, the setup process of 2FA is crucial; difficult setup procedures might even discourage users from using 2FA at all [2]. However, setup procedures ideally have to be done only once and can be improved.

Considering the authentication phase, several studies demonstrated the usability of OTPs via SMS [2, 11, 16], OTP generators [11, 16], tokens [6, 10, 14] and smartphone apps [2, 11, 16] while pointing out shortcomings that are possible to correct. An example is the research by Das et al., who successfully demonstrated usability improvements of the YubiKey [10]. After an initial study, they refined the YubiKey and demonstrated its improved usability.

Even though the studies mentioned above clearly demonstrated that the authentication phase can be usable, it has also been shown that user experience-related aspects and the user's context play an essential role when adopting 2FA [10, 14, 16, 17, 31]. Participants in studies of tokens, for instance, were not willing to use a token because they feared losing it [10, 14]. Further, participants in studies voiced an unwillingness to set up and carry around single-purpose extra devices [16, 17, 31]. Some OTP generators ran out of battery when needed [17]. While participants could successfully authenticate, the duration of the procedure was perceived as too long [6, 11, 32], especially when doing multiple authentications as part of a daily routine [17].

Summary. 2FA can be usable, but the usability of the setup and authentication phase is not enough. This paper investigates 3D-Auth as an alternative tangible authentication concept. First, we investigated what kind of items users might want to use for authentication. Second, we prototyped the most common shapes and investigated how users interacted with them over a week. Our study considers the participants' contexts and interviews them about 2FA integration in their daily routines.

3 Study I: User-Defined Tangibles

In our first investigation, we wanted to find out what kind of 2FA tangibles users want to use in their daily life, specifically investigating RQ1 (*What kinds of tangibles do users design for 2FA?*). For this, we conducted an online user study with 226 participants. During the study, participants were asked to configure their tangibles as a form of authentication. For this, we implemented a design pipeline, where participants were guided through a design process by picking several tangible properties, as detailed below.

Study Procedure. First, after reading and accepting our consent form, we explained the concept of a 2FA tangible, how it works and possible interactions to the participants in textual form. After a trial run with ten participants, the description texts were refined, and illustrative pictures were added to foster a better understanding. We further added a quiz to the end of the familiarisation part to help participants by testing their understanding. These items served as attention checks in case participants failed them multiple times following the guidelines of Prolific.

Second, participants designed their ideal 2FA tangible following a mock design pipeline. First, they designed the physical appearance of the tangible in free text. Next, they provided specifications on the colour and size of the tangible. Then, they were asked about the desired number of interactions

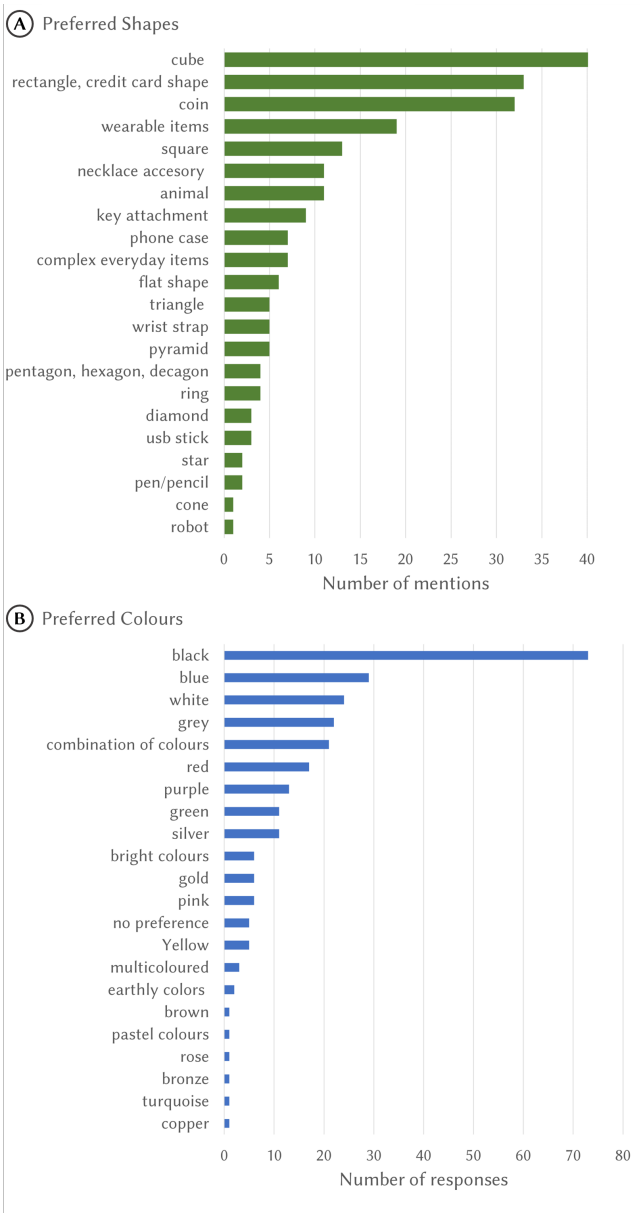

Figure 1: The preferred shapes (a) and colours (b) stated by the participants of the online study.

based on the interaction space with the five interaction categories from Marky et al. [18] and to provide the specific interactions they would like to perform with their tangible. Another attention check was carried out here.

In the last step, participants were asked for demographics including age, gender, origin, and answers to the affinity of technology scale [13]. After the participants completed all question sets, they were redirected to the survey platform for reimbursement.

Recruitment & Participants. We recruited 233 participants using the Prolific online platform[1]. Seven of them failed more than one attention check resulting in 226 valid datasets. Of them, 129 identified as male, 90 as female, and seven identified as self-described. Their mean age was 27 (*min* = 18, *max* = 58, *SD* = 8). Participants were compensated with an hourly rate of an equivalent of 11 US dollars.

Limitations. Like most online studies, our investigation has several limitations among them are wrong self-assessments and biased answers due to social acceptability. It might be challenging for participants to make judgements about configuring 2FA tangibles without the possibility of exploring them physically or having experience interacting with them. The sample might not be representative of the entire population of potential 2FA tangible users. Hence, our results should be validated through future in-depth studies with more heterogeneous samples.

3.1 Results

We analysed the collected designs, colour, and size descriptions by an inductive categorisation approach [19] where two researchers independently grouped the participants' answers into clusters of designs, colours, and sizes. Disagreements were resolved in a review meeting.

Tangible Design. Participants suggested a wide variety of shapes and colours for possible 2FA tangibles (see Figure 1). Possible sizes were clustered into three groups: small (1-3 cm, N=56), medium (4.5-6 cm, N=59), or large objects (8-10 cm, N=42) in quite equal proportions. Instead of giving absolute terms, they linked their favourites to objects they already knew. For example, 25 participants chose size 10 cm as they associated it with a pencil shape they might want to use. Other participants linked their ideas to relative statements, such as *"a thumb"* (P111) or *"a penny"* (P140). Considering the design, three main clusters of tangibles emerged:

(1) Standalone Tangibles: Most participants (N=107) described a standalone tangible for authentication. More specifically, the description from the participants based on the specified shape and properties was a 2FA tangible that is neither connectable nor insertable into another everyday object, such as a wallet. Interestingly, participants preferred rather generic shapes, such as cubes (N=43), squares (N=13), or pyramids (N=5), instead of more complex geometries. The majority of those, who preferred a more complex shape, described animals (N=11). Participants, for instance, envisioned the following 2FA tangibles:*"It could be a cube, that I can play around and rotate the cube so that the side with the internal authentication object would be known only by me."*, **P408**.

[1] https://www.prolific.co, last-accessed 1-February-2023

"I like the idea of having a collection of animal authentication objects. For my taste, probably a cat.", **P118**.

Even though participants were not specifically asked to justify their choices, some of them did so by mentioning portability aspects, such as P149 who wrote *"It would like a pencil but a bit smaller so that I could always carry it with me and use it with no difficulties."*, **P149**.

(2) Wallet-Fit Tangibles: Participants specifically named tangibles that fit into their wallets or pockets (N=65), either credit card-shaped (N=33) or coins (N=32). Participants described these, for instance, as follows:

"[...] the size and shape of a typical credit card.", **P208**.

"It should look like a coin, so it's comfortable to carry in my wallet, pocket, etc.", **P087**.

"A card that displays numbers or codes that could be kept in one's wallet.", **P180**.

(3) Connectable Tangibles: Connectable tangibles are the smallest category (N=54). Those tangibles are somehow connectable to either another daily object in the form of key rings (N=9), and phone cases (N=7) or to the human body as a wearable (N=38). Even though participants were not asked for in-depth justifications, most participants that described connectable tangibles mentioned that they want an object that ideally passes as something that is not linked to authentication:

"'bullet' or 'pendant shaped', such that it could pass as a necklace to someone who didn't know what it was.", **P040**.

"I would prefer a small object, such as a ring or bracelet. Preferably something I can wear.", **P191**.

"The goal for me is to be very discreet, when people see the object they won't know it is an authentication object, so it has to be design/decorative, for example, a phone case, if you touch it at specific points in a specific order it will unlock, but no one will notice.", **P232**.

Interactions. When asked for the preferred number of interactions, 35.71% of participants stated two interactions. A slightly smaller share (34.52%) prefers one interaction. The remainder of the participants stated willingness to use three (16.07%), four (5.95%), five (5.95%), six (1.19%), or ten interactions (0.59%).

In addition, participants were asked to choose interactions for their designed tangible (multiple answers and different interaction combinations were possible). 39.88% of the preferred interactions were touch-based. This was followed by configuration with 24.92% and arrangement (20.23%). Only a few participants preferred assembly (11.43%) and augmentation (2.34%). In 1.17% of the interactions, participants added their descriptions with image recognition, voice interaction, and pinning.

4 Design & Prototype Implementation

In this section, we describe the tangible design process that we followed to develop the 2FA tangibles for Study II. While we initially considered using the 3D-Auth items presented in the literature [18], those did not match the user preferences voiced in Study I. Therefore, we designed a new set of 2FA tangibles that is optimised for mobile usage.

Designing 2FA Tangibles. We used the data set collected in Study I as a basis for designing tangible for Study II. First, we filtered out designs without a flat surface or those that were too small to embed the capacitive material. Then, we developed the first set of candidates based on the interactions preferred in the online study. We filtered out the interactions augmentation and assembly because the majority of participants had concerns about using them on the go. Augmentation might be difficult due to the need for water or some other external media. Assembled tangibles result in more individual objects that might be lost. Finally, we matched the list of candidates with the three tangible categories from the online study to propose several candidates for each category.

All tangibles were designed to fit into pockets, purses and wallets. The static authentication structure was a square shape with an embedded dot structure for each tangible, representing the ownership factor. The dynamic parts and designs are as follows (see also Fig. 2), each interaction serving as the knowledge factor:

1) Wallet Category: Credit card with touch interaction. This tangible has the approximate dimensions of a standard credit card (85mm $\times$ 55mm), with the exception of the thickness, which was made larger (3mm) to ensure that no touches on non-conductive material were registered. To authenticate with the tangible, users place the item on their phone and perform a sliding motion over a circle of ten dots printed with the conductive material. First, the users start touching the top dot and then clockwise to the fifth dot (180°). Then, they move anti-clockwise to the second dot to the left (270°). Finally, the user touches the square structure. This was to mimic using a safe lock.

2) Standalone Category: Cube with arrangement interaction. This tangible has the style of a die (20mm $\times$ 20mm $\times$ 20mm), which many people surveyed suggested in their responses, with each side containing a different number of pips of conductive material. The side of the die that would usually have the number one had the square that encodes the ownership factor. To authenticate, the users touched the smartphone with different sides of the item following the sequence four, one (ownership factor), four, and two. Each of the numbers denotes the number of dots on the respective die side.

3) Connectable Category: Key-chain with configuration interaction. This tangible is a combination lock, with ten possible digits for each layer and three total layers, each assembled onto a central axis. Each layer is 30mm $\times$ 30mm $\times$ 5mm, with the central axis 23mm tall. To authenticate, users align the three layers matching the number sequence one, three, and seven, similar to the way one would interact with a combination lock, and then touch the item to the phone. Additionally, the central axis was created with conductive material to serve as a 'control', allowing for the phone screen to read unsuccessful attempts.

Prototypical Authentication App. To facilitate the collection of information and allow users to experience performing login authentications with a 2FA tangible, we created a mock authentication app (see Appendix A.4.) for Android that simulated the experience of unlocking a remote account (e.g., emails or online banking) which might currently be unlocked via an OTP received, for instance, by SMS or authenticator app. For this, we implemented the following functionality that also serves as the basis for Study II: First, the app offers a tutorial for each tangible to allow users to learn without requiring a demonstration. Second, the app recognises the interactions using each of the 2FA tangibles to provide a proper authentication experience. If participants could not authenticate, the app allows skipping the process. After the authentication or authentication skip, the app prompts the participants to answer a short survey consisting of different questions depending on the authentication terminal state. Third, the app collects the required data and transmits it to our cloud database via Firebase messaging. Forth, the app receives notifications, so we can nudge participants to authenticate throughout the day. The notification can be snoozed to serve as a reminder to participate in the study at least once a day.

We envision this concept as part of an app that requires login via 2FA where no switch of app or device is needed, hence the mock authentication app was intended to allow a simulation of the need for authentication during the day.

5 Study II: 2FA Tangibles in the Wild

Based on the results of Study I, we conducted a follow-up study to investigate RQ2 (*How do tangibles for 2FA perform in the user's daily lives? What are obstacles and challenges introduced by such novel tangibles?*) For this, the tangibles detailed prior were distributed to 15 participants and used for one week to unlock a remote account.

Collected Data. The data collected during the study by the app fell into two categories: First, *authentication data*, consisting of the time taken to complete the authentication, the timestamp the authentication took place, the number of attempts required, whether the authentication was successful, whether the user skipped the authentication and the user's participant number. Second, the app collected *survey data*. This differed slightly in wording depending on whether the user succeeded, failed, or skipped. Each survey collected information on the user's location when they performed the authentication (multiple choice), what issues the users had, if any (multiple choice), whether they would like to perform this authentication in a similar setting (single choice) and why (open text), and further feedback (open text, optional). All survey questions are provided in Appendix A.1.

Study Procedure. The study consisted of an initial meeting, a one-week usage period (between one and three authentications per day), and an exit meeting including an interview. During the initial meeting, participants were met either in-person or online, with 15 minutes allocated:

First, participants were informed about the concept of 2FA tangibles, and what they would be required to do over the week. Then, informed consent was obtained.

Second, each participant was assigned one tangible at random[2], and installed the study app on their device. The information for the first start of the app (participant number and model type) was given to ensure data was collected correctly. Upon setup completion, participants were asked to navigate to the app tutorial page to learn how to use their assigned model. The participants were then given an opportunity to use the app, including performing mock authentications and survey responses. Finally, the participants were asked to press the 'Begin the Study' button in the app, as well as schedule their exit meeting for one week later.

Upon completing this initial phase, participants were to go about their lives as usual, ensuring their 2FA tangible was with them and being aware of notifications from the study app. When a notification was received, participants were to open the app and authenticate with the tangible, with the option to skip if they did not have access to the tangible or for any other reason. After each authentication, the survey mentioned above was issued in the app to collect responses regarding the participant's experience using the 2FA tangible during that authentication.

Reflection Interview. Once the week had concluded, participants were met again, with this meeting taking place online. Thirty minutes were allocated for this meeting and proceeded as follows: The participants were reminded of the study's purpose and asked if they had any questions. A short survey was issued to collect demographic information. Then, a recorded interview was carried out to obtain information about the participant's experience using the tangible over the past week, their first impressions, non-assigned tangibles, and what they would like to see in the future for this method of authentication. Time was also allotted to allow participants to give any further information or ask final questions. For the

[2]To ensure an equal share of participants for each object, we had 15 objects in total, meaning that five participants interacted with each object.

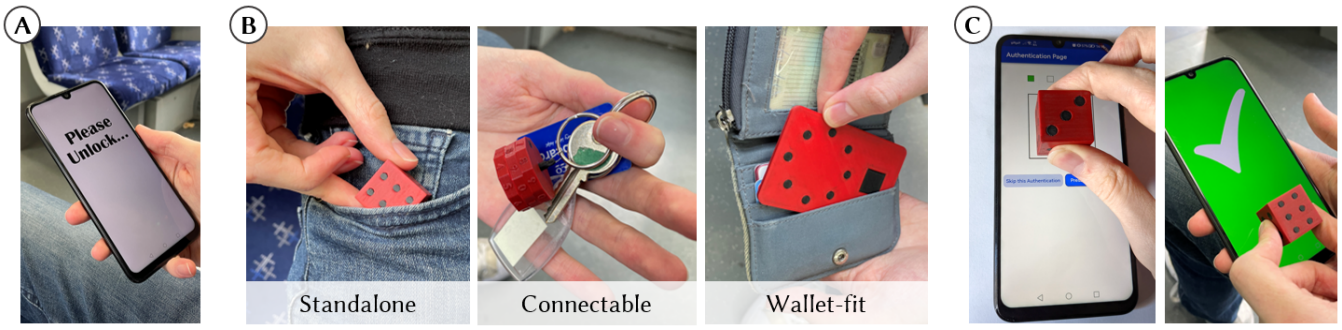

Figure 2: Tangibles used in Study II. To authenticate, users take out their smartphone (a), configure their tangible object (b) and then hold it against the touchscreen (c). For bigger depictions and screenshots of the app, we refer to Figure 3 in Appendix A.4.

full interview script, the reader is referred to Appendix A.2. Finally, the participants were reimbursed with an Amazon voucher with an equal value of roughly 25 US Dollars.

Pilot Study. Before the actual study, we conducted a week-long pilot study (N=3) to investigate the feasibility of the study design, as well as to detect any issues with the tangibles that impacted their performance over the course of extended use. Each participant was assigned one tangible. The tangibles were also intensively tested by the research team. The issues discovered during the study were related to the app developed and the tangibles created. One problem brought up was the lack of guidance and feedback offered by the app, to alleviate this an improved tutorial page was added, along with visual status hints for each tangible during authentication attempts. The cube model was also chosen to receive a progress indicator during the authentication attempts as this tangible required multiple touches to the screen.

Data Analysis. Before the analysis, all audio recordings were transcribed. Next, two researchers familiarised themselves with the data by reading the transcripts repeatedly. A shared codebook was proposed and finalised in a review meeting. The codebook is provided in Appendix A.3. Then, one author analysed all transcripts and applied the codebook reaching saturation after the 10th participant. After that, the second researcher further analysed the entire coding to validate and mark all the codings they disagreed with. Finally, the two researchers came together in a final discussion meeting to agree on a final coding. After this, both researchers grouped the codes into five main themes.

Recruitment, Participants. We recruited 15 participants through mailing lists and word-of-mouth. They were aged 26.1 years old (*min* = 21, *max* = 39, *median* = 24, *SD* = 5.43) on average. Ten identified as male, with the remaining five identifying as female. An affinity for technology interaction survey [13] was also issued, resulting in an average ATI score of 4.48 (*min* = 3.22, *max* = 5.89, *median* = 4.67, *SD* = 0.84). Hence, the sample had a rather high affinity for technology.

Limitations. We had a rather tech-savvy sample that might have overly welcomed the usage of tangibles. Consequently, our results can only serve as a first step towards understanding the design choices and interaction experiences of users. Hence, our results should be validated through future in-depth studies with more heterogeneous samples. The participants used tangibles randomly assigned to them. Hence, these tangibles were not personalisable. Because of that, participants might have received a tangible that they would not design themselves. Further, our tangibles were optimised for mobile usage considering the size. Because the size of a tangible might also be dependent on the device used, such as smartphones or tablets, future work should investigate the full process, including tangible design, personalisation, fabrication and usage as a whole including other sizes than those investigated by us. Further, participants used the tangible for one week. The results regarding ease of use and fun should be taken with a grain of salt since there might be a novelty effect. Consequently, future work should investigate longer usage periods. Finally, participants did not use the 2FA tangibles for their real accounts. This might have impacted their perceptions of the concept. Future work should investigate a realistic use case where 2FA tangibles protect real assets. However, our participants used the tangibles on their own devices and in different areas of their daily environments.

Ethical Considerations. All studies reported in this paper were reviewed and approved by our ethics board. The participants were informed via a consent form that participation is voluntary and that they could abort at any time without consequences. The collected data cannot be linked to individual participants. Audio data was transcribed before analysis, and the consent forms were kept separate from all other data. The recognition of tangibles would have been more accurate, and smaller tangibles would have been possible if par-

ticipants' mobile devices were rooted. This, however, would have exposed the private devices of the participants to security risks. In coordination with the ethics committee, we decided to simulate the security properties of 2FA tangibles with a low-resolution recognition to not expose the participants to security risks by rooting. Further, we used mock accounts for unlocking, because we did not want to impact the security of the participants' personal accounts. Further, the tangibles were printed with PLA plastic that, on the one hand, keeps its shape but, on the other hand, is soft enough to not injure participants or leave any kind of scratches on their devices.

6 Study II: Quantitative Results

Overall, the participants performed 197 authentications over the week and completed the related survey 163 times.

Authentication Success: The participants reported eleven unsuccessful authentication attempts. All of them were because the tangible was not available.

Duration: An authentication started once the participant indicated in-app that they have their tangible ready and ended when a complete attempt was recognised. For the cube, the mean duration of an authentication attempt was 15.5 seconds (*min* = 7.8, *max* = 31.7, *SD* = 5.38), for the card, it was 11.3 seconds (*min* = 5.4, *max* = 43.9, *SD* = 5.47) and for the pendant 8.6 seconds (*min* = 2.7, *max* = 44.8, *SD* = 8.09).

Location & Usage Intention: Participants were asked to indicate the location where they authenticated and whether they would like to perform an authentication in a similar setting to capture their usage intention. In total, 59 authentications (36.2%) were reported as *at home*. Of those, 64.4% answered affirmatively when asked about willingness to authenticate in a similar setting. For instance, P13 said they enjoyed the *"interactive way to authenticate items"*, while P4 liked that they could *"just have a place where [they] keep the authentication device"*. Five authentications (3.1%) were performed in *private places* different from their own home, with four participants stating usage intention. Eighty authentications (49.1%) were performed *at work* with 47.5% usage intentions. For example, P2 found that it *"takes too long"* to use for work, P5 also stated that it *"takes too much precision to operate"*. However, P4 felt that *"if [they] could keep the object just in the office ready, it would be handy"*. Six authentications (3.7%) were done *in transit* with 16.7% (N=1) usage intention. P8 stated that it was *"impractical whilst travelling"* to use the tangible, with P7 elaborating that they *"felt overwhelmed on the subway and couldn't concentrate on the activity"*. Finally, ten authentications (7.4%) were done in *public* with a 40% usage intention. P4 found they were *"not near... where [they] kept the [tangible]"* and found difficulty authenticating while P8 appreciated the aspect of *"security in a public place"*.

7 Study II: Qualitative Results

Overall, our participants welcomed the concept of 2FA tangibles for use in their daily lives. This section reports our results grouped into themes identified by the thematic analysis.

7.1 Security Perceptions

The participants liked that 2FA tangibles add a layer of security to their accounts. Metaphors also played an important role in defending from shoulder surfers or conveying security.

Security Benefits are Valued: Most of our participants commented on the security of 2FA tangibles, specifically considering that they are physically separate from the smartphone:

"This [tangible] combined with logging in to feels more secure. It does feel very secure. Like to have all the steps of having to have the thing and know the password for it and know which account it was linked to.", **P3**.

"For the most part I like the idea of the security being there. [gives examples] There is a bit of extra security because you've obviously got to have the token with you and then know how the token works. So, it's like an in-built two-factor authentication basically that requires you to have something and know how to use it.", **P8**.

The perceived benefit also impacted the participants' usage intentions. Most of them wanted to use 2FA tangibles for important accounts, such as financial services where 2FA is required and text messages with one-time passwords or apps were not considered secure enough. Further, participants frequently brought up the idea of using a 2FA tangible as a backup in case a password or other form of authentication mechanism was not available for them:

"[...] banking for example. Whenever I do, I tend to do financial things at home where I'm like, not in a hurry and I'm pretty stationary there, so in cases like that, for example, I would actually say yeah, why not? That could be good. A use case, I think, yeah.", **P12**.

Metaphors are Considered: Some participants linked their security perceptions to the specific tangible design that was considered as a metaphor. The cube was perceived as less secure than the card. The card, on the other hand, was perceived as less secure than the pendant. Participants stated that the pendant is already mentally associated with security and would prefer it based on the visual appearance. That was somewhat similar for the card shape. Here, some participants associated it with a credit card or they associated the interaction with the card with opening a safe by a security dial:

"I think the pendant [is my favourite] because it mimics already a lock. I think it makes you think that it's more secure than a dice where dice is almost just like a toy object.", **P4**.

The metaphors could also specifically be used to defend participants better. For instance, bystanders might associate cards and pendants with security. A few participants were concerned that bystanders might shoulder-surf them because they know they are currently authenticating. However, participants that used the cube did not voice such a concern because the cube is a neutral object. These comments also match some statements of participants in the online survey and related studies [17] who mentioned preferring benign everyday objects over something with a connection to security:

"I didn't really feel all that strange to be doing the authentication in public either like people probably just thought I was playing a game or something since it was just a red and black dice. I felt like it didn't really stand out much.", **P7**.

7.2 Positive Aspects

Our participants voiced further positive aspects after interacting with the tangibles for a week. In sum, the participants welcomed the possibility to customise the tangible and the option to self-fabricate it. The interaction was perceived as fun and easy to use. Finally, the tangible interactions were easy to memorise.

Customisation is Welcomed: Several participants particularly liked that 2FA tangibles are personalisable in a way. Hence, users can buy something different from a standardised off-the-shelf tangible. One participant even welcomed the independence from manufacturers since such tangibles could be 3D-printed by the users. Sample comments are:

"I like the basic concept of another factor for authentication that I can own. I'm a YubiKey user myself, so I guess I'm kinda well used to something like that and well. I thought about it and the idea of having a token that you can maybe customise even I think it's that's pretty cool for future ideas.", **P12**.

"I mean theoretically if I had issues with the model and it broke for something like a YubiKey, I'd need to go to the supplier and get a new one. But for something like this model, it's relatively easy to go off and print it for yourself and I feel that idea is really nice. It doesn't have any kind of really special technology that kind of limits it to not being able to be manufactured at home, and I feel that that's also a cool feature of it.", **P5**.

Using Tangibles is Fun: Several participants stated that authentication with the tangibles during the study period was fun for them. P3 gave a quite representative statement:

"I think it was quite successful. I just kept the card in my wallet and so I always had it with me when the thing went off. I enjoyed it generally. I just really enjoyed it, but it never really occurred to me in the past to like to have a physical thing that physical keys could be used for online accounts and so I like the idea that you can have this.", **P3**.

These results, however, should be taken with a grain of salt because the 2FA tangibles were only used for a week. Consequently, we cannot rule out potential novelty effects at this state of usage.

Tangibles are Easy-to-Use: Several participants considered the tangible and also the app as easy-to-use. They also considered that when we showed them the other tangibles that they had not used over the week. Some participants even commented on the tangibility:

"I felt quite good, I use MFA apps, so you know, where you use a PIN code, so you just copy and paste that. This is kind of the same idea. You basically just typing out a PIN, but a different method. So yeah, it was quite good.", **P13**.

"I like the idea that we don't have to even type something. This is the main advantage I think, in my opinion, that we don't type in anything. Any numbers, so.", **P11**.

Interactions are Memorable: Some participants said that the interaction with the tangibles was very easy to memorise for them compared to other traditional authentication methods:

"I think the pin and the system will be more memorable than a password for sure, if you had given me a password to log in for the week, I'd give you a month before I know what it was.", **P3**.

"Yeah, it's quite easy. I mean the PIN code was static, so it wasn't as if you have to remember like a randomised number each time, so just remember where it is in the dice and put in and you're finished.", **P12**.

7.3 Experienced and Perceived Issues

Even though the participants reported many positive aspects, they also told us about issues encountered during the week. These issues included forgetting the tangible at home, further design-related issues that might impact the interaction, problems with slippery tangibles, usability issues, and theoretical issues based on the fact that the 2FA tangibles are designed to work with touchscreen devices only.

Forgetting the 2FA Tangible: Some participants voiced issues based on the portability of 2FA tangibles. In particular, they were concerned about forgetting the tangible somewhere or the tangible being stolen and consequently being locked out of their accounts:

"Yeah, although it seems more secure, but still I have to carry this extra model. Uh, this is my concern. Probably I will. Sometimes I will. Forget to take it with me if it is integrated so I don't have to worry about whether sometimes probably, I will forget. So, just had to carry the model with me. So, if it is integrated then it should be very nice.", **P11**.

"I did not attach it to any of the things that I regularly take with me when I leave home. And because I had a week where I went to different places with different bags, I actually did not have it with me a lot of the time.", **P2**.

Issues with Shape or Size: Other participants had no issue with forgetting the tangible but voiced concerns based on the shape and size that it might impact portability. The cube, for instance, had too sharp edges for some participants, making them concerned about getting hurt while accidentally sitting on it in their pockets. While that did not happen during our study, the tangible's geometry was perceived to have a high impact on portability. One participant feared that sharp edges might even damage the smartphone screen, which is not possible due to the softness of the used PLA printing material:

"So, I generally like dice. [...] That's most of what I liked about it. Uhm. I think it's not that handy because you can't really transport it. Uh, because it has very sharp edges and so on, and it's pretty big for a device.", **P9**.

"So the first thing my partner commented on when I took the thing home and tried to authenticate at home was like, yeah, but you have to touch it onto your phone and if you like if it is dirty because it's coming out of your bag, what if you are leaving scratches in your phone display?", **P2**.

Further, the size of the tangible was frequently mentioned. E.g., the cube was too big to match the habit of not carrying anything besides the smartphone of P7. Another example was P9, who did many interactions with their smartwatch, but the cube was too big for that. The concerns voiced by these participants were not linked to the concept of 2FA tangibles in general but rather to the specific dimensions that tangibles could or should have:

"So because of the size of the object, the display of the Smartwatch is too tiny for that kind of authentication. So doing it with a smartphone as the smartphone is the main device when accessing services, I would say yes. No, I don't want to use it on my smartwatch.", **P9**.

Slippery Tangibles: Some participants reported issues using the tangible with one hand on the go because the tangible slowly slid away. P10 gave a representative comment:

"When I used it at home, it would be much easier for me than to use it outside, because you need to have the phone placed at the table or any non-moving object and you need to press down the authentication object on it. So, for example, if I was at, uh, in a bus or on any uh, movable. Uh, sorry, in any uncontrolled situation, I don't think the authentication method will have worked.", **P10**.

Interoperability Aspects: An issue that was not actively experienced by the participants but was frequently mentioned in the interviews was the interoperability of 2FA tangibles with other devices. Since the tangibles investigated by us are limited to touchscreen devices, some participants wished for better interoperability, including laptops or personal computers without touchscreen functionality.

"Generally for interacting with a computer, I don't feel it's the best for interaction with, a non-touchscreen device just due to how it's implemented. Theoretically, if it also worked on the trackpads as well, perhaps it could be used for authentication with laptops.", **P5**.

Usability Issues: Moreover, the participants also reported usability issues that were mostly linked to the way the tangibles need to be used. These participants mainly had issues when using the tangibles on the go:

"From a user perspective, it's very inconvenient [...] it's not something which is easy, you can't do it while holding the telephone free and I've had my best success rate when fixating or putting the phone on a desk something and setting the authentication object on it and which basically means you have to sit somewhere [...] And if you're not in a situation which allows this, some kind of setting it's just difficult.", **P1**.

"Usability wise [it] is like, if you're just sitting nice, it's nice and easy to get out if you're not moving and as I say it then becomes a factor of the location.", **P8**.

8 Discussion & Limitations

This section first discusses the security properties of 2FA tangibles including a path to realistic tangibles that are secure. Next, we focus on the portability issues voiced by the participants and options to solve them. This is followed by a discussion of the tangible shapes, sizes as well as considerations thereof and limitations of our investigations. Finally, we use this discussion to motivate a user-centred fabrication pipeline for 2FA tangibles.

What About Security? First and foremost, security is the most important aspect of authentication [3]. While the tangibles used in our investigation can only provide limited security, as their authentication patterns are quite simple, it was sufficient for investigating how 2FA tangibles integrate into daily life from an HCI perspective. To create secure items, the following challenges need to be solved:

Completely 3D-printed tangibles: We 2FA tangibles should be completely 3D-printed, we need a way to *increase* the resolution of the authentication pattern to offer a large password space by encoding a more significant number of different interactions. This requires access to the capacitive raw data [27, 28] which currently is not possible on non-rooted devices. The tangibles used in our study were limited to the Android API that only offers access to ten touchpoints – one for each finger – at once. Having access to this data allows the recognition of a larger number of smaller dots in closer distances to each other. Hence, device manufacturers need to provide more powerful APIs that give more options to developers. While this challenge may be technologically solvable in the long run with device manufacturer support, the question arises whether fully 3D-printed tangibles are indeed an ideal solution for realising 2FA. Having fully 3D-printed tangibles has several benefits: (1) tangibles can be printed in one pass

without the need to configure any electronics, (2) the tangibles are passive, removing the need for energy sources, and (3) shapes can be personalised. The second two aspects were also mentioned by our study participants, with one person even liking the idea of 3D printing the tangible at home because it provides independence from suppliers. Since the current recognition technology is not yet accurate enough, we would also like to argue for partially 3D-printed tangibles.

Partially 3D-printed tangibles: The personalisation benefits from 3D-printing could be combined with other technology, e.g., NFC tags or passive tokens [35]. The general idea is that tangible interactions are used to activate the token. Currently, YubiKey tokens need a simple touch making the possession of the token sufficient to impersonate the user. To address this issue, we envision a series of more complex interactions to trigger authentications. Even though this has to be verified by future work, such tangibles would likely have similar security perceptions as those in our study. Further, they would solve the interoperability issues voiced by several participants since such tags are not limited to touchscreens.

In summary, the security of 2FA has priority but has yet to be realised by standalone 3D printing. Therefore, we recommend combining the usability and UX benefits of 3D-printed 2FA tangibles with the security benefits of other technology, such as NFC tags.

Addressing Portability Issues. Many participants voiced concerns about the portability of 2FA tangibles. Some participants even forgot the tangibles at home and could not access them for some time during our study. These concerns were mainly linked to standalone tangibles (the cube in Study II) that can neither be connected to another object nor fit into a wallet or pocket. Moreover, several participants stated they were unwilling to do security-critical interactions, like banking transactions, on the go unless it is urgent. Consequently, they would not need tangibles with great portability. Based on that, we recommend integrating the location of intended tangible use in the design pipeline, such that portability can be considered. Portable tangibles should either be small enough to easily fit in a pocket or wallet or offer an option to be connected to another object, like a key chain. Shape properties should be considered, such that users do not get injured from too sharp edges while having a tangible in the pocket.

Another interesting aspect is that users are not limited to a specific material that works in any environment. As suggested by one of our participants, users might have a static tangible on their desk or at another place at home for most interactions and a mobile tangible that they keep in their wallet in case they have to authenticate on the go. Since this contrasts study results in the literature where study participants did not want multiple items [31], future work has to validate this. However, related work specifically investigated one-time password generators with a specific form factor and size. Hence, these results might not transfer to 2FA tangibles.

Tangible Shapes and Sizes. The majority of the over 200 participants in our first study chose simple geometric shapes. Animals, like cats or dogs, formed the most complex shapes. The participants of the main study revealed more in-depth considerations of that. Tangibles with sharp edges might hurt users when they sit on them or look for them in their pockets. Further, complex shapes might be more likely to break and do not fit well into pockets or wallets. The sizes of tangibles were also closely connected to portability. Highly portable tangibles should be small, but those used at home could be bigger, with some participants in the online study even designing tangibles of 10 cm size that could cover their entire smartphone screen. Based on that, we conclude that the shape of 2FA tangibles should be simple. This does not mean that simple geometric shapes are the only solution; animals and other shapes that people like could also be simplified. As for the size, again, the environment in which the user intends to use the tangible should be carefully considered.

What About the Friction? Friction [20] is a construct from habit research denoting anything that might constrain a human in doing a specific task. Friction might be beneficial to get rid of unhealthy habits but might be an obstacle to creating new ones. Throughout the reports of the participants, we found two ways how 2FA tangibles impact the participants' habits. Either the tangibles resulted in more friction because they did not match user habits, or they helped them establish new and helpful security habits that they have not had before.

We further investigated the usage over the course of a week to also find out whether participants could establish a habit of using the tangibles and how the tangibles might interfere with other habits. As detailed in the results section, only two participants struggled with bringing the tangible with them because it was their habit to carry only their smartphones and wallets. Both participants interacted with the cube that neither fits in a wallet nor can it be attached to another object. When confronted with the other models during the interviews, the participants were more positive, yet honestly stated that their habits would likely prevent them from using external devices for authentication for two reasons: First, participants stated to prefer performing security critical tasks in a static environment, for instance, at home. Second, they were used to purely digital solutions, e.g., one-time passwords by text messages, that they would need more time to create the habit of interacting with 2FA tangibles. The remainder of the participants struggled less. They either had the tangibles all the time in their pockets, on their key rings, in their wallets or placed them in a dedicated spot, for instance, on their desk to, be available for authentication. They were used to carrying more when they left home, so the additional tangible did not add more friction. Two participants even went on vacation during our study and brought the tangibles with them without issues. Since the tangibles better matched the habits of these participants, they had fewer issues in performing the study

tasks on the go and even welcomed this new security habit.

In sum, if users have the habit of not carrying any specific objects besides their smartphones regularly, then 2FA tangibles create more friction. For users that already carry additional objects, like a purse or key rings, 2FA tangibles are connected to an existing habit and are available when needed.

9 User-Centred Fabrication Pipeline

Based on our results and the discussion, we envision a user-centred fabrication pipeline where the users design personalised 2FA tangibles. Per step, we highlight either possible realisations or provide guidance for future work.

1) Usage Type. First, the users choose whether they want to use their 2FA tangible in a static or mobile fashion because this has implications for the tangible design, shape, and size. This step does not require further investigations, however, future work should investigate what users primarily choose as environment type.

2) Usage Context. Next, users indicate the specific surrounding environment. E.g., static environments might be their home which has other implications for security compared to a shared workspace. Here, a list of possible specific environments is required. Our study participants stated to use the tangibles at home, at work, on the go, or in other private environments. Further, security implications of these specific environments are needed. At home, for instance, shoulder surfing might be less of an issue. These security implications should be the basis for an environment-specific security model that helps users choose suitable interactions later on.

3) Device. The device the user wants to use the tangible for impacts the tangible's shape and further properties. For instance, if the tangible needs to be recognised on a touchscreen, the tangible requires at least one flat surface. If the tangible would be used with a PC, it might need a USB connector. While the requirements for standalone 3D-printed devices and USB keys are partly known, future work should investigate the requirements for mixed tangibles that allow a custom shape with integrated sensors.

4) Interactive Choice of Tangible Shape & Size. Since the shape impacts the tangible size, users should be able to choose these two properties at the same time interactively. The pipeline should have a list of suggested shapes based on the previous two choices. For static environments, a standalone tangible might be the first suggestion, whereas wallet-fit or connectable tangibles might be better for mobile users.

5) Interaction(s). Once the shape and size are known, users suggested that they want to first decide on the number of authentication interactions. For this, the pipeline should give a recommendation based on the security properties of the specific environment. Using this information, the pipeline can automatically calculate possible interactions that can be performed with the chosen shape. Especially the last step requires an algorithm that takes a 3D shape as input and calculates possible interactions based on it, offering another opportunity for future work.

6) Manufacturing. The users now choose to fabricate the tangible themselves, go to a public maker space or order it from a manufacturer. This is based on the specific components required to fabricate a tangible.

7) Backup. Finally, all design decisions are stored in an encrypted file to allow revoking and recreating the 2FA tangible in case it was lost or broken.

Exploration of this fabrication pipeline and its evaluation with users is a mission for future research toward user-friendly tangible 2FA that can be customised to the user and use case.

10 Conclusion

2FA tangibles are a potentially viable alternative for solving UX and security issues of currently available 2FA mechanisms. To investigate 2FA tangibles, we first simulated a simple fabrication pipeline where 226 participants designed tangibles by describing their size, colour, shape, and possible interaction. Participants' designs mainly consisted of simple geometric shapes that either described a) standalone objects, b) tangibles that can be connected to another object, or c) tangibles that fit into wallets or pockets.

For each of those categories, we prototyped one tangible and let 15 participants use our tangibles in the wild to perform authentications over one week. From our study, we learned that the participants welcome the security benefit provided by the 2FA tangibles. Further, they considered the specific tangible design as a metaphor that could support security perceptions or obscure the connection to security. The main issues that participants experienced during the study were connected to portability, but those participants would prefer using a tangible in a static environment, such as their desk at home. Based on the results of our investigations, we first discussed possibilities to address the shortcomings and how 2FA tangibles impact user habits. Finally, we proposed a user-centred fabrication pipeline that can be used by the users to design personalisable 2FA tangibles. Overall, 2FA tangibles are a promising solution to make 2FA easier to use, fun and more secure, but future work is needed to realise fabrication pipelines and investigate them with users.

Acknowledgments

This work was supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972. Furthermore this work was co-funded by the EPSRC(EP/V008870/1).

References

[1] Jacob Abbott and Sameer Patil. How mandatory second factor affects the authentication user experience. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–13, New York, NY, USA, 2020. Association for Computing Machinery.

[2] Claudia Ziegler Acemyan, Philip Kortum, Jeffrey Xiong, and Dan S Wallach. 2fa might be secure, but it's not usable: A summative usability assessment of google's two-factor authentication (2fa) methods. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 62(1):1141–1145, 2018.

[3] Joseph Bonneau, Cormac Herley, Paul C. Van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 553–567, Piscataway, NJ, USA, 2012. IEEE.

[4] Swati Chaudhari, SS Tomar, and Anil Rawat. Design, implementation and analysis of multi layer, multi factor authentication (mfa) setup for webmail access in multi trust networks. In *Proceedings of the International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, pages 27–32, Piscataway, NJ, USA, 2011. IEEE.

[5] Stéphane Ciolino, Simon Parkin, and Paul Dunphy. Of two minds about two-factor: Understanding everyday FIDO u2f usability through device comparison and experience sampling. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 339–356, Berkeley, CA, US, August 2019. USENIX Association.

[6] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. "it's not actually that horrible": Exploring adoption of two-factor authentication at a university. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, CHI '18, pages 456:1–456:11, New York, NY, USA, 2018. ACM.

[7] Federal Financial Institutions Examination Council. Authentication in an internet banking environment. *Retrieved June*, 28:2006, 2005.

[8] Alexei Czeskis and Juan Lang. Fido nfc protocol specification v1.0. FIDO Alliance Proposed Standard, 2015.

[9] Sanchari Das, Andrew Dingman, and L. Jean Camp. Why johnny doesn't use two factor a two-phase usability study of the fido u2f security key. In *Proceedings of the International Conference on Financial Cryptography and Data Security (FC)*, pages 1–20, Cham, Switzerland, 2018. Springer.

[10] Sanchari Das, Gianpaolo Russo, Andrew C. Dingman, Jayati Dev, Olivia Kenny, and L. Jean Camp. A qualitative study on usability and acceptability of yubico security key. In *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*, STAST '17, page 28–39, New York, NY, USA, 2018. Association for Computing Machinery.

[11] Emiliano De Cristofaro, Honglu Du, Julien Freudiger, and Greg Norcie. A comparative usability study of two-factor authentication. In *Proceedings of the Workshop on Usable Security*, pages 1–10, 2014.

[12] J. Dutson, D. Allen, D. Eggett, and K. Seamons. Don't punish all of us: Measuring user attitudes about two-factor authentication. In *Proceedings of IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, pages 119–128, Piscataway, NJ, USA, 2019. IEEE.

[13] Thomas Franke, Christiane Attig, and Daniel Wessel. A personal resource for technology interaction: Development and validation of the affinity for technology interaction (ati) scale. *International Journal of Human-Computer Interaction*, 35(6):456–467, 2019.

[14] S. Ghorbani Lyastani, M. Schilling, M. Neumayr, M. Backes, and S. Bugiel. Is fido2 the kingslayer of user authentication? a comparative usability study of fido2 passwordless authentication. In *Proceeedings of the IEEE Symposium on Security and Privacy (SP)*, pages 268–285, Piscataway, NJ, USA, 2020. IEEE.

[15] Maximilian Golla, Grant Ho, Marika Lohmus, Monica Pulluri, and Elissa M Redmiles. Driving 2fa adoption at scale: Optimizing two-factor authentication notification design patterns. In *Proceedings of the USENIX Security Symposium*, USENIX Security 21, pages 109–126, Berkeley, CA, US, 2021. USENIX Association.

[16] Kat Krol, Eleni Philippou, Emiliano De Cristofaro, and M Angela Sasse. "they brought in the horrible key ring thing!" analysing the usability of two-factor authentication in uk online banking. In *Proceedings of the Workshop on Usable Security*, USEC 2015, Reston, VA, USA, 2015. Internet Society.

[17] 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 Trans. Comput.-Hum. Interact.*, 29(5), oct 2022.

[18] Karola Marky, Martin Schmitz, Verena Zimmermann, Martin Herbers, Kai Kunze, and Max Mühlhäuser. 3d-auth: Two-factor authentication with personalized 3d-printed items. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–12, New York, NY, USA, 2020. Association for Computing Machinery.

[19] Philipp Mayring. *Qualitative content analysis: theoretical foundation, basic procedures and software solution*. Social Science Open Access Repository (SSOAR), Klagenfurt, 2014.

[20] Asaf Mazar, Geoffrey Tomaino, Ziv Carmon, and Wendy Wood. Sustaining sustainability: Lessons from the psychology of habits. *PsyArXiv Prepr*, 2020.

[21] Martez Mott, Thomas Donahue, G. Michael Poor, and Laura Leventhal. Leveraging motor learning for a tangible password system. In *Extended Abstracts of the CHI conference on Human Factors in Computing Systems*, CHI EA '12, pages 2597–2602, New York, NY, USA, 2012. ACM.

[22] Martez Mott, Thomas Donahue, G. Michael Poor, and Laura Leventhal. Leveraging motor learning for a tangible password system. In *CHI '12 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '12, page 2597–2602, New York, NY, USA, 2012. Association for Computing Machinery.

[23] Ahmad R. Pratama and Firman M. Firmansyah. Until you have something to lose! loss aversion and two-factor authentication adoption. *Applied Computing and Informatics*, 2021.

[24] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. A usability study of five two-factor authentication methods. In *Fifteenth Symposium on Usable Privacy and Security*, SOUPS 2019, Berkeley, CA, US, 2019. USENIX Association.

[25] Jun Rekimoto. SmartSkin: An Infrastructure for Freehand Manipulation on Interactive Surfaces. In *Proc. SIGCHI Conference on Human Factors in Computing Systems*, CHI '02, pages 113–120. ACM, 2002.

[26] Joshua Reynolds, Trevor Smith, Ken Reese, Luke Dickinson, Scott Ruoti, and Kent Seamons. A tale of two studies: The best and worst of yubikey usability. In *Proceedings of the IEEE Symposium on Security and Privacy (SP)*, pages 872–888, Piscataway, NJ, USA, 2018. IEEE.

[27] Martin Schmitz, Florian Müller, Max Mühlhäuser, Jan Riemann, and Huy Viet Viet Le. Itsy-bits: Fabrication and recognition of 3d-printed tangibles with small footprints on capacitive touchscreens. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[28] Martin Schmitz, Jürgen Steimle, Jochen Huber, Niloofar Dezfuli, and Max Mühlhäuser. Flexibles: Deformation-Aware 3D-Printed Tangibles for Capacitive Touchscreens. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, CHI '17, pages 1001–1014, New York, NY, USA, 2017. ACM.

[29] DUO Security. Security tokens. https://duo.com/product/trusted-users/two-factor-authentication/authentication-methods/security-tokens, 2019. [Online; accessed: 22-August-2019].

[30] Teddy Seyed, Xing-Dong Yang, Anthony Tang, Saul Greenberg, Jiawei Gu, Bin Zhu, and Xiang Cao. Cipherchard: A token-based approach against camera-based shoulder surfing attacks on common touchscreen devices. In *Human-Computer Interaction – INTERACT 2015*, page 436–454, Berlin, Heidelberg, 2022. Springer-Verlag.

[31] Jake Weidman and Jens Grossklags. I like it, but i hate it: Employee perceptions towards an institutional transition to byod second-factor authentication. In *Proceedings of the Annual Computer Security Applications Conference*, ACSAC 2017, pages 212–224, New York, NY, USA, 2017. ACM.

[32] Catherine S. Weir, Gary Douglas, Martin Carruthers, and Mervyn Jack. User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security*, 28(1-2):47–62, 2009.

[33] Catherine S. Weir, Gary Douglas, Tim Richardson, and Mervyn Jack. Usable security: User preferences for authentication methods in ebanking and the effects of experience. *Interacting with Computers*, 22(3):153–164, 2009.

[34] Shota Yamanaka, Kunihiro Kato, Tung D Ta, Kota Tsubouchi, Fuminori Okuya, Kenji Tsushio, and Yoshihiro Kawahara. Sheetkey: Generating touch events by a pattern printed with conductive ink for user authentication. 2020.

[35] Yubico. Yubikey neo. https://www.yubico.com/products/yubikey-5-overview/, 2019. [Online; accessed: 25-August-2022].

A Material Study II

A.1 In-App Questions

When login was successful:

- Where are you at the moment?
  - at home
  - at work
  - in transit (e.g., bus or train)
  - in a public place (e.g., restaurant, park)
  - in a private place (e.g., home of a friend)
  - other (please specify)
- Did you experience any issues with authentication?
  - yes
  - no
- What kind of issues did you experience?
  - I had to look for the item
  - I needed multiple attempts
  - The timing of authentication was not convenient
  - Other (please specify)
- Would you like to perform 3D authentication in a similar setting in your daily life?
  - yes –> why?
  - no –> why not?
- Do you have any additional feedback? (free text)

When login was not successful:

- Where are you at the moment?
  - at home
  - at work
  - in transit (e.g., bus or train)
  - in a public place (e.g., restaurant, park)
  - in a private place (e.g., home of a friend)
  - other (please specify)
- What kind of issues did you experience?
  - I had to look for the item
  - I needed multiple attempts
  - The timing of authentication was not convenient
  - Other (please specify)
- Would you like to perform 3D authentication in a similar setting in your daily life?
  - yes –> why?
  - no –> why not?
- Do you have any additional feedback? (free text)

When login had to be skipped (when pressing the skip login button):

- Where are you at the moment?
  - at home
  - at work
  - in transit (e.g., bus or train)
  - in a public place (e.g., restaurant, park)
  - in a private place (e.g., home of a friend)
  - other (please specify)
- What kind of issues did you experience?
  - I had to look for the item
  - I needed multiple attempts
  - The timing of authentication was not convenient
  - I accidentally skipped
  - Other (please specify)
- Would you like to perform 3D authentication in a similar setting in your daily life?
  - yes –> why?
  - no –> why not?
- Do you have any additional feedback? (free text)

A.2 Interview Script

Thanks for participating in our study. During the past week, you have used one of the 3D-printed authentication items. In this interview, we would like to learn about our experience to improve the items to create better authentication mechanisms in the future. We are interested in your opinion, there are no right or wrong answers.

- How was the last week when you interacted with the items?
- Were there any issues? If yes, which ones? (Talk about each issue and ask what could be improved, separate between app and item)
- What did you like about the items?
- What didn't you like? How could that be made better in your opinion?
- Here are two alternatives that we designed, have a look at them. Compared to your item, would you prefer one of the alternatives? Why (not)?
- The 3D printed items can be printed in any shape, if you could decide, what would you prefer and why?
- Assuming that your dream item would be possible, would you like to use it in your daily life or rather something else like SMS notifications or a USB Key? Why (not)?
- Is there anything else that you would like to tell us?

A.3 Codebook

Table 1: Codebook used to analyse the interviews.

Category	Code	Description
Security Perceptions	separated_token	security benefit by a separated token
	metaphor	security consideration of a metaphor
	eyes_free_interaction	tangibles might be used in secret without looking at it
	observing	considerations based on presence of bystanders
	scalability	secures many devices
Positive Aspects	customisation	tangibles can be customised or self-fabricated
	interaction_fun	tangibles are fun to use
	ease_of_use	tangibles are easy to use
	memorability	interactions are easy to remember
Experienced Problems	tangible_forgotten	tangible was forgotten, e.g., at home
	tangible_size	problems based on size
	tangible_design	problems based on shape
	no_recognition	tangible was not recognised by app
	usability	Manufacturer is responsible
Considered Issues	tangible_might_be_forgotten	tangible might be forgotten
	reset_needed	tangible needs reset after login
	tangible_too_big	tangible perceived too big
	tangible_design	design not liked
	interoperability	tangible limited to touchscreen device
Ideal Tangible	thin	tangible should be thin
	small	tangible should be small
	everyday_item	tangible should be everyday item
	durable	tangible should be durable
	connectable	tangible should be connectable

A.4 Prototypes and Screenshots

In this section, we provide screenshots of the app used in Study II and pictures of the 2FA tangibles.

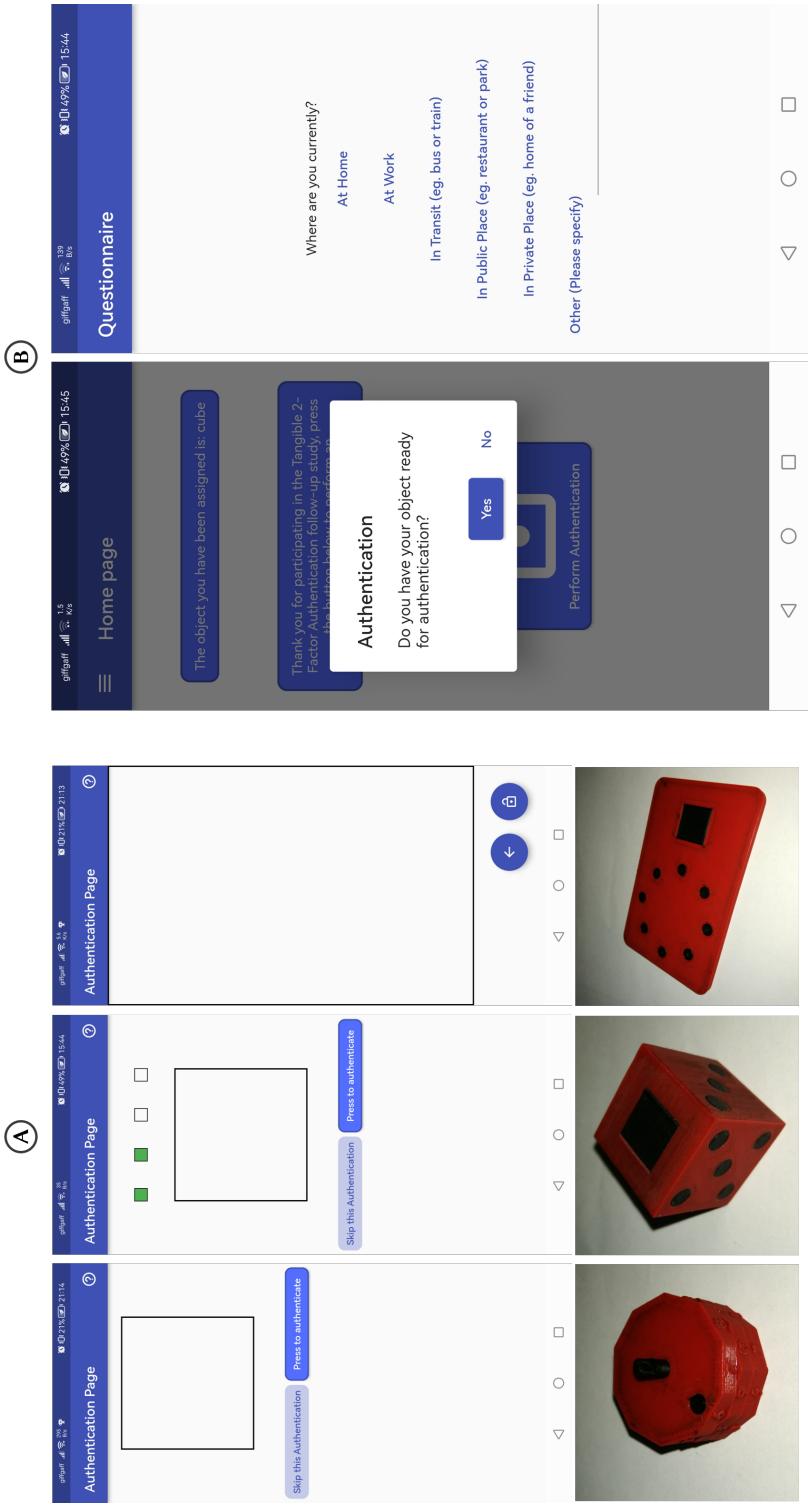

Figure 3: This figure depicts our three developed prototypes as well as screenshots of the app used in the study. Part A shows the specific login screen for each tangible whereas part B shows the screen of the survey after the authentication.