Carrying Secrets: Exploring Security Perceptions of Physical Transport Devices

Sarah Delgado Rodriguez
sarah.delgado@unibw.de
University of the Bundeswehr Munich
Munich, Germany

Swantje Kastrup
swantje.kastrup@unibw.de
University of the Bundeswehr Munich
Munich, Germany

Maximilian Wagner
wagner.maximilian@posteo.de
LMU Munich
Munich, Germany

Eva Hemauer
hemaurev@hu-berlin.de
HU Berlin
Berlin, Germany

Florian Alt
florian.alt@ifi.lmu.de
LMU Munich
Munich, Germany

Marco Gutfleisch
marco.gutfleisch@ifi.lmu.de
LMU Munich
Munich, Germany

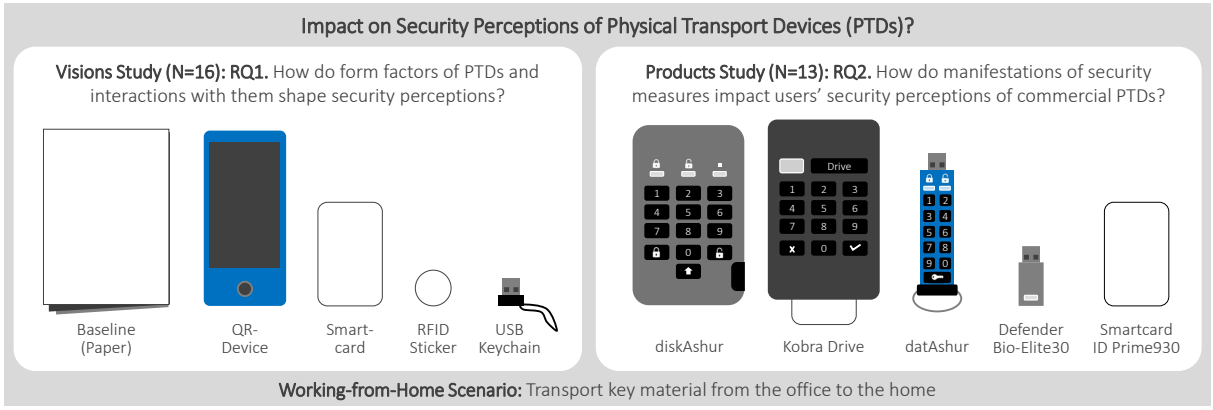


Figure 1: We present empirical findings on the impact of form factors, supported user interactions, and implemented security measures on users' security perceptions of physical data transport devices (PTDs). In two complementary studies, we evaluated (1) five prototypes derived from users' visions of secure PTDs and (2) five commercially available secure PTDs.

Abstract

Physical transfer of sensitive data (e.g., on a flash drive) remains common but exposes users to unique risks, including loss, tampering, and substitution. Security in such contexts depends on users' ability to assess these risks correctly. However, it remains unclear how design cues impact security judgments. Addressing this gap, we explore how security perceptions are shaped by user interactions, form factors, and security features of physical data transport devices with two complementary studies. First, we elicit user visions of secure physical data transport, instantiate recurring concepts in five prototypes, and evaluate them in a user study (N=16). Second, we evaluate five commercially available devices (N=13) to surface the impact of security and authentication methods. Our findings suggest that usability correlates with trust, tangibility increases perceived security, and users focus on availability and integrity-related considerations. We discuss divergences between perceptions and plausible threats, and derive takeaways for the design and adoption of future physical transport devices.

CCS Concepts

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

Keywords

security perception, tangible security, data transport

ACM Reference Format:
Sarah Delgado Rodriguez, Swantje Kastrup, Maximilian Wagner, Eva Hemauer, Florian Alt, and Marco Gutfleisch. 2026. Carrying Secrets: Exploring Security Perceptions of Physical Transport Devices. In *25th International Conference on Mobile and Ubiquitous Multimedia (MUM '26), December 01–04, 2026, Glasgow, United Kingdom.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3861188.3861222

This work is licensed under a Creative Commons Attribution 4.0 International License.
MUM '26, Glasgow, United Kingdom
© 2026 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-2791-7/2026/12
https://doi.org/10.1145/3861188.3861222

1 Introduction

While most usable security research focuses on software systems and online threats, many sensitive activities still require physical data transport. Whether for "air-gapping" critical infrastructure or managing cryptographic keys, users routinely transfer sensitive data using physical devices such as USB flash drives [24, 37]. Such physical data transfer introduces a unique threat vector: the device leaves the safety of managed networks or secured hardware, shifting the security boundary to the physical transport device (PTD) and its user. Correspondingly, these devices face threats during transit such as loss, theft, tampering, or substitution. Mitigating these risks often requires secure user behavior (e.g., physical safeguarding), which critically depends on understanding the underlying risks [1, 7, 45]. However, security perceptions are shaped by media, prior experiences, and metaphors, which are often incomplete or misleading [5, 22, 46–48]. For example, users of end-to-end encrypted messaging applications such as Signal often fail to correctly verify encryption keys due to misunderstandings of underlying security concepts [39].

While security perceptions of digital interfaces have been extensively studied, our understanding of physical hardware remains limited. Research on physical authentication devices shows that form factor, build quality, and interaction mechanisms influence perceived usability and trustworthiness [29, 36, 38]. However, unlike PTDs, physical authentication devices do not transmit generic data but store or generate device-bound cryptographic credentials for specific authentication operations (e.g., challenge-response or signing). Thus, differences in users' goals, functionality, and interaction limit the applicability of these findings to PTDs. A systematic investigation of how design cues, interaction patterns, and implemented security features shape security perceptions in physical data transport is therefore missing. We address this gap by investigating users' security perceptions across various PTDs within a realistic working-from-home scenario through two research questions:

- **RQ1 – Form & Interactions:** How do form factors of physical transport devices (PTDs) and interactions with them shape security perceptions?
- **RQ2 – Implemented Security Measures:** How do manifestations of security measures (i.e., connectivity and authentication mechanisms) impact users' security perceptions of commercial PTDs?

To disentangle design cues and interaction patterns from implemented security features, we explore these questions through two complementary mixed-methods studies. First, we elicited users' visions of a secure PTD and evaluated five corresponding prototypes in a lab study (N=16) to analyze form- and interaction-related security perceptions without constraining participants to existing commercial designs. Second, we evaluated how implemented security features, such as authentication and protection mechanisms, affect perceptions of five commercial secure PTDs (N=13). Figure 1 provides an overview of the PTDs we compared in each study.

Our results suggest that perceived usability and trust align. Availability- and integrity-related considerations shape preferences for form factors, materials, and shapes, while confidence in commercial devices is particularly influenced by the presence and visibility of authentication mechanisms. Based on our findings, we derive takeaways for designing and adopting future PTDs and contrast participants' perceptions with threat models for physical data transport to identify mismatches between anticipated and plausible risks.

Contribution Statement. We contribute to human-centered security research by (1) conducting two complementary studies exploring how design cues, interaction patterns, and implemented security features shape security perceptions of PTDs and (2) deriving concrete takeaways for future research, manufacturers, and decision-makers.

2 Background & Related Work

Understanding how users form security perceptions requires considering the relationship between actual and perceived security. However, security understanding is inherently complex, involving multiple stakeholders (e.g., developers, users, and attackers) and reasoning about threat and system models, attacks, and countermeasures [45]. This complexity makes security perceptions prone to misconceptions, as frequently observed in related work.

2.1 Security Misconceptions

Users' reasoning about security is often incomplete, inconsistent, or inaccurate. Camp [9], for example, described five dominant metaphors for communicating security and privacy that each capture only parts of the underlying problems and thus support protection against only subsets of possible attacks.

Wash [47] identified eight "folk models" of security threats among North American home computer users, including beliefs of being too insignificant to be targeted by hackers. These models shaped decisions such as installing anti-virus software, making backups, or following security advice. Kauer et al. [30] replicated this work in Germany and identified additional models, including beliefs that viruses or hackers are governmental actors. Later survey work by Wash [48] shows a complex relationship between beliefs and behavior: weak beliefs about viruses or hackers were associated with less protective behavior, while strong beliefs – regardless of content – were associated with more action. Hence, "more-is-better" measures of security knowledge fail to capture the diversity of real-world beliefs.

Media – particularly television and film – also shape security perceptions. Fulton et al. [22] report common tropes, including hackers targeting high-value victims, obvious attacks, fragile encryption, or simple solutions to complex problems. Baig et al. [5] replicate and extend this work with technically trained participants, who identified unrealistic portrayals but remained influenced by media and misinformation. Finally, many works identify misconceptions regarding specific security topics, particularly encryption [3, 4, 14, 17, 50].

Taken together, misconceptions occur frequently across cybersecurity domains, shape security decisions and behaviors, and are influenced by diverse factors.

2.2 Perceptions of Physical Authentication Devices

More closely related are works investigating users' perceptions of physical authentication devices (PADs) and how design features shape them. Nanda et al. [36] identified compatibility, support,

quality, and simplicity as important for positive perceptions. Design and build quality (i.e., "interference") affected perceived reliability, accessibility, usefulness, and ease of use. Participants also expressed clear preferences for specific form factors (e.g., smaller vs. larger devices) and raised concerns about loss due to size. Jongkil et al. [29] later confirmed the importance of interference, while Cristofaro et al. [13] found perceived trustworthiness and usability to be related. In contrast, Tischer et al. [43] found that adding labels or physical keys to USB flash drives did not increase the likelihood of them being plugged in. Users instead often showed altruistic intentions, suggesting that such cues did not reliably impact risky behavior.

Payne et al. [38] investigated acceptance of a hypothetical token-based authentication system (Pico). Acceptance depended on familiarity with PADs and their design, with participants generally preferring a card-shaped prototype. Preferences reflected ease of carrying and using the device, including its shape, size, and interactions, with dual-purpose or integrated designs reducing inconvenience. Moreover, physicality increased perceived personal responsibility for loss, theft, or malfunction and corresponding security, reliability, and interruption concerns.

Marky et al. [34] explored tangible interactions with customizable 3D-printed PADs for two-factor authentication, finding positive attitudes toward tangible authentication and good memorability of authentication secrets. Building on this work, Turner [44] found a preference for pocket-sized standalone devices over wallet-fit or connected devices in a formative survey (N=226). Field-study participants described tangible interactions as fun, easy, and memorable, while device size, the risk of forgetting them, and unreliable performance reduced willingness to adopt them.

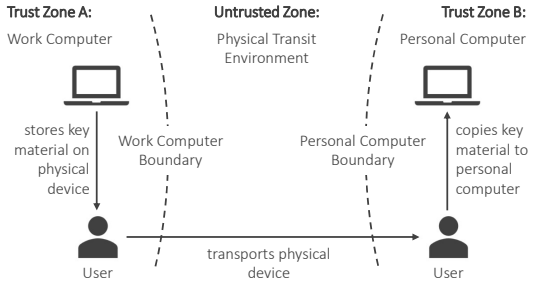
In sum, design cues shape users' perceptions and adoption of PADs. However, these findings may not transfer to PTDs because users' goals differ (i.e., authentication vs. secure data transport), potentially resulting in different motivations, needs, and perceptions. We, thus, extend existing research to PTDs and provide empirical insights into how implemented security measures and design cues influence perceived security.

3 Research Approach

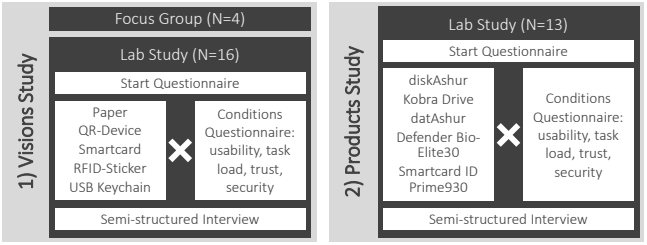
3.1 Research Context

In the following, we describe a working-from-home scenario that we presented to participants of both studies to (1) situate the study tasks in a relatable and easy-to-grasp context (i.e., working from home) and (2) to ensure that participants have a similar perception of the sensitivity of the data they are transporting (i.e., a cryptographic key required to access work-related data). We also systematically categorize the potential risks of physically transporting sensitive data with a threat analysis using the STRIDE model [31, 32].

3.1.1 Working-from-Home Scenario. Bob's employer uses a security system that allows communication from outside sources (e.g., employees working from home) only through an encrypted connection. Moreover, the symmetric encryption key must not be sent over the internet, as this is deemed insecure, and changes every few days. So Bob transmits the current symmetric key in his office onto a PTD. He then takes this device home, where he uses it to encrypt his data exchange while working.



(a) System model and security boundaries for the physical transport of keys between a trusted work computer (Trust Zone A) and a personal computer (Trust Zone B) via an untrusted transit environment.



(b) We conducted two complementary empirical studies: the *visions study* and the *products study*. Both studies included an initial questionnaire, a hands-on phase in which participants tried each device and evaluated it through condition-specific questionnaires, and a final semi-structured interview.

Figure 2: Visual representations of our research context and the process we applied to answer our research questions.

3.1.2 Threats to Physical Data Transport. As illustrated in Figure 2a, we describe threats to the transport of cryptographic keys via a physical device between two trusted endpoints (Trust Zones A and B) through an untrusted environment. We assume the technical integrity of both the work and home office computers (i.e., operating systems and hardware are considered secure). However, this trust does not extend to their physical environments. We account for risks emerging from shared or semi-public spaces, including human-centric threats like visual observation or unauthorized access.

S – Spoofing. An adversary may *replace the transport device or its peripheral components with a visually identical malicious counterfeit*, for example, during a brief window of opportunity, such as unauthorized access to a hotel room ("Evil Maid" attack), in public transit, or in *semi-trusted environments*, such as open-plan offices or shared housing.

T – Tampering. Even a brief absence of the user in shared or semi-public spaces may provide a window for an adversary *to manipulate stored data, corrupt the file system or modify the hardware,* even without permanently removing the PTD. Since the PTD is offline during these phases, it typically lacks active integrity monitoring or file-locking mechanisms found in networked systems. Hence, tampering may lead to a silent system compromise. Even with robust verification, tampering may still result in a successful Denial-of-Service by obstructing the key transfer.

R – Repudiation. An adversary or negligent user could *deny responsibility for the loss, theft, or unauthorized access* of the PTD. As PTDs typically lack auditing capabilities, such as immutable logs or timestamps, the chain of custody during transport cannot be reliably reconstructed. Consequently, an adversary could access the data (e.g., replacing key material) without leaving forensic artifacts.

I – Information Disclosure. An adversary could access the confidential key material through physical and observational vectors particularly in semi-trusted environments, such as *loss or theft*, *visual observation* (e.g., shoulder surfing during PIN entry), or wireless attacks using proximity readers – similar to skimming attacks [41].

D – Denial of Service. An adversary or environmental factors could cause the *permanent unavailability* of the key material at the destination by stealing, destroying, or damaging the PTD within the untrusted physical transit environment. Physical hazards (e.g., water, heat, or magnetic fields) and mishandling can likewise prevent successful key transfer – whether due to targeted sabotage, environmental hazards, or human error.

E – Elevation of Privilege. An adversary could modify or replace the PTD to function as a Human Interface Device (HID), executing 'BadUSB' attacks [33] to compromise the host system. However, as the primary asset is the static key material rather than the destination endpoint, host-level escalation is considered out of scope.

3.2 Research Process

As illustrated in Figure 2b, we applied a two-step research approach to answer our research questions.

First, the *visions study* investigated how users envision PTDs without constraining them to existing security mechanisms (e.g., encryption), providing broader insights into security perceptions and their translation into design features [38]. A formative focus group with 4 participants informed the selection of devices with different form factors and transfer interactions, which 16 additional participants evaluated during complete key transfers in a lab study.

Second, the *products study* investigated the impact of implemented security features using five commercial PTDs with state-of-the-art AES-XTS encryption with a 256-bit key or AES-based secure messaging (i.e., AES-256 session keys), covering different form factors and authentication mechanisms. Thirteen participants transferred keys with each device and evaluated their perceptions.

Both lab studies used a within-subject mixed-methods design, combining established scales, own Likert items, and semi-structured interviews. This enabled comparisons of form factors while controlling for individual differences in security perceptions. We counterbalanced device order to reduce learning and fatigue effects.

3.2.1 Ethical Considerations. Low-risk human-subject studies (i.e., with tasks similar to regular office jobs, no additional stressors, and not targeted at particularly vulnerable populations) such as those presented here – are exempt from IRB approval under our local legal regulations and institutional requirements. Hence, we instead adhered to our institution's ethical guidelines. In particular, we ensured that participants received a detailed explanation of the data being collected, the study's purpose, the estimated duration, and the compensation before deciding whether to participate in our studies. Participants were also provided a consent form that again detailed the previously mentioned information, as well as information about the voluntary nature of participation and the option to withdraw at any time without negative consequences. In addition, we deleted all potentially identifiable data directly after finishing the study (fingerprint) or after finalizing the data analysis and compensation procedure (contacts, audio, and video). Participants in our lab studies were compensated at 10€ per hour, as recommended by our university's ethics guidelines.

3.2.2 Data Collection & Analysis. In our user studies, we collected both quantitative and qualitative data.

We transcribed all audio recordings manually and consulted videos when clarification was required. Two researchers first familiarized themselves with the transcripts from both studies. Taking an inductive approach, each researcher independently developed an initial codebook by coding all interviews from one study each. The researchers then compared, refined, and merged both codebooks into a unified one (Appendix C) that covered themes from both studies. Subsequently, each researcher re-coded the interviews they had initially analyzed using the unified codebook and reviewed the other researcher's coding to identify inconsistencies, which were discussed until consensus was reached.

We analyzed quantitative data descriptively and assessed normality using Q–Q plots and Shapiro–Wilk tests [40]. For approximately normal distributions, we used repeated-measures ANOVAs with Greenhouse–Geisser corrections [23] and Holm-corrected paired-sample t-tests [28] for post hoc comparisons. For non-normal distributions, we used Friedman tests [21] and Holm-corrected Wilcoxon signed-rank tests [49]. We examined associations between user interaction (i.e., usability and workload) and security perceptions (i.e., trust and additional Likert items) using repeated-measures correlations [6] with Holm corrections. Given our exploratory approach, we report descriptives, effect sizes, and confidence intervals alongside inferential analyses.

3.2.3 Limitations. Our formative focus group included only four participants and was not intended to be exhaustive, but to identify readily elicited user visions. To still ensure that participants' input was meaningful, we contrasted it with Payne et al. [38] before deriving the PTD visions informing the visions study apparatus (see also Section 2.2). Both lab studies relied on self-reported data, subject to social desirability and recall bias. Moreover, our samples were small (N: 16 and 13), male-dominated, young, and geographically limited, restricting generalizability, statistical power, and precision. Accordingly, sensitivity analyses determined minimum detectable effect sizes for paired t-tests (Cohen's d) and repeated-measures correlations, with degrees of freedom defined following Bakdash and Marusich [6]. We report these results at the beginning of both quantitative result sections (Sections 4.3.1 and 5.2.1). We further report descriptives, effect sizes, and 95% confidence intervals (CI) and apply Holm corrections [28] for multiple comparisons. Nonetheless, our findings require confirmation with larger samples.

	not attached	attached
inserted	smartcard	USB keychain
nearby	QR device	RFID sticker

(a) We applied a 2x2 attachment style vs. transfer style matrix to choose a subset of participants' visions.

Gender	Age		ATI	SA6	SeBIS	PTT
9 male	$mean = 27.38$	mean	3.67	3.18	3.64	3.28
7 female	$std = 2.60$	std	0.90	0.61	0.49	0.46

(b) Demographics of visions study participants.

Table 1: Contextual information regarding the visions study.

4 Visions Study

4.1 Formative Focus Group

To inform the device selection, we conducted a formative 90-minute online focus group moderated by an experimenter.

The experimenter first presented the working-from-home scenario (Section 3.1.1) and the focus group's goal. Participants then discussed guiding questions (Appendix A.1) and documented ideas on a Mural board. Finally, they categorized their ideas by originality and feasibility using a Now-How-Wow matrix [12]. One researcher transcribed the recordings and combined them with the Mural entries. A second researcher reviewed everything for completeness.

4.1.1 Elicited Visions. We recruited four computer science graduates for the focus group (3 male, one female). Participants were $median = 30$ years old (range: $27 - 33$) and rated their IT expertise with $median = 4$ on a 1-5 scale. Participants envisioned aesthetic, small, inconspicuous, and distinguishable PTDs, noting that *"for everything larger than a smartphone, one would have to think hard if it still has a use"* [P2]. Devices could be attached to everyday objects or users (e.g., keychains, jewelry, implants) or resemble existing devices (e.g., USB flash drives, smartcards, OTP tokens, YubiKeys). Suggested transfer mechanisms included wireless (Bluetooth, NFC, RFID) and wired (USB) connections, QR codes or barcodes, and patterns using color, light, audio, vibration, or physical structures *"like Braille, or just something 3D [...] like a [wax] seal"* [P3]. Participants suggested additional authentication factors and tamper resistance and raised concerns about observing or intercepting key transfers.

4.1.2 Prototype Selection. Consistent with related work [38], participants envisioned small, inconspicuous PTDs that could be attached to objects or users or carried in a pocket. The key transfer is triggered by proximity or physical connection. Based on these concepts, we implemented four prototypes covering diverse interaction methods for the subsequent lab study (Table 1a; Appendix A.2).

4.2 Method

Our study comprised five secret key transport *conditions*: the four PTDs from Table 1a and an analog, manual baseline condition. The study was conducted in a vacant office with two desks and notebooks simulating an *office* and *home office*. Both notebooks had a camera and USB port and were connected to a self-built smartcard/RFID reader (Appendix A.2). A simple GUI guided participants through the key transfer using each of the following PTDs:

Baseline (Paper): Participants received a DIN-A4 sheet containing the key and typed it into a text field.

Smartcard: We used a white ID-1 smartcard. Participants inserted it into a reader and waited for the transfer to complete.

USB keychain: We used an Intenso Micro Line USB flash drive with keychain attachment (18 x 15 x 7 mm, USB-A). Participants plugged it into a USB port and selected the corresponding folder through our GUI.

QR device: We used an Android smartphone with a custom app. To convey its role as a dedicated key transport device, we enabled airplane mode, disabled notifications and app switching, and covered it with tape. Participants transferred keys to the device by scanning a QR code and back by presenting the displayed code to a camera.

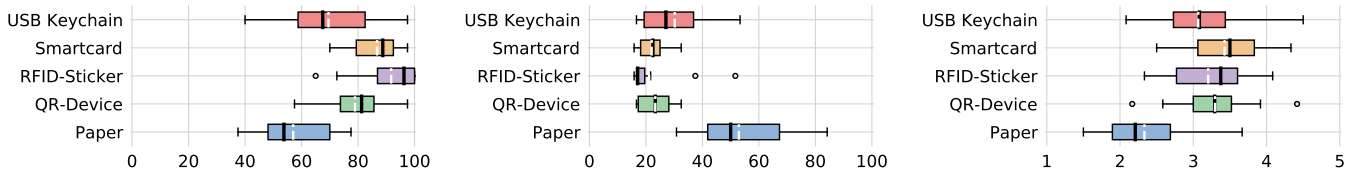
RFID sticker: We used a white NFC sticker with an NTAG216 chip (diameter: 30mm). Participants held it near the reader and waited for the transfer to complete.

4.2.1 Procedure. Participants first completed a *start questionnaire* covering demographics, work-from-home frequency, affinity for technology interaction (ATI [20]), security attitudes and behaviors (SA-6 [19]; SeBIS [18]), and propensity to trust technology (PTT [35]). The experimenter then presented the working-from-home scenario (Section 3.1.1) and briefly introduced each PTD. Participants performed test interactions to familiarize themselves with the task and GUI. In each condition, they transferred a key from the office PC to the PTD, transported it to the home-office desk, and transferred the key to the home-office PC. Afterwards, participants completed a *condition questionnaire* comprising the System Usability Scale (SUS) [8], Raw NASA Task Load Index (RTLX) [27], Human–Computer Trust Scale (HCTS) [25, 26], and additional Likert items on perceived security (Appendix A.3). We counterbalanced condition order using a Latin square. Finally, we conducted a semi-structured interview comparing the user experience and perceived security across PTDs. The study lasted about 60 minutes.

4.2.2 Recruitment & Participants. We recruited 16 participants using university mailing lists and chats. 9 identified as male and 7 as female (see Table 1b). Their mean age was $mean = 27.38$, and all participants had a university degree and resided in Germany. Their affinity for technology interaction ($ATI = 3.67$) was similar to scores of the German general population [20]. However, their security attitudes score ($SA6 = 3.18$) and security behavior intentions were slightly below the averages reported in related works [15, 19]. Most participants worked > 4 times a week from home ($N = 9$).

4.3 Results

4.3.1 Condition Questionnaires. For brevity, we describe only statistically significant differences here ($\alpha = 0.05$). Appendix A.4 provides additional details, Figure 3 shows answer distributions and Table 2 lists participants ratings per condition. With 16 participants and 5 repeated measurements per participant, our study had 80% power to detect paired-samples effects of at least Cohen's $d_z = 0.75$ and repeated-measures correlations of at least $|r| = 0.34$. Moreover, given our small sample, we interpret quantitative differences primarily as directional patterns, especially where post-hoc comparisons were not statistically significant.



(a) System Usability (SUS) **(b) Task Load (RTLX)** **(c) Human-Computer Trust (HCTS)**

Figure 3: Standard scale scores comparing the different prototypes evaluated during the visions study. Medians are shown through a bold black line and means through a dashed white line.

User Interaction: Usability & Workload. A repeated-measures ANOVA identified significant differences among conditions in usability (i.e., SUS scores; $F(4, 15) = 24.68$, $p < 0.001$). The usability of the *paper* was rated worst and significantly lower compared to the *QR device* ($p = 0.001$), *RFID sticker* ($p < 0.001$), and *smartcard* ($p < 0.001$). The usability of the *RFID sticker* was rated best and significantly higher than the *QR device* ($p = 0.010$) and the *USB keychain* ($p = 0.007$). The *smartcard's* usability was also rated significantly better than the USB keychain ($p = 0.014$). A Friedman test revealed significant differences in the reported workload between conditions ($\chi^2(4) = 40.70$, $p < 0.001$, Kendall's $W = 0.64$). The *paper* induced the highest task load and was rated significantly more demanding than the *QR device* ($p < 0.001$), *RFID sticker* ($p < 0.001$), *smartcard* ($p < 0.001$), and the *USB keychain* ($p = 0.001$). Moreover, a Friedman test revealed significant differences in participants' perceptions of how easily the prototypes are transportable ($\chi^2(4) = 14.75$, $p = 0.005$, Kendall's $W = 0.23$). However, post hoc pairwise comparisons did not reveal any significant differences between the conditions after Holm correction.

Security Perceptions: Trust & Own Items. A repeated-measures ANOVA revealed significant differences in participants' trust in the devices (i.e., overall HCTS scores; $F(4, 15) = 11.36$, $p < 0.001$). Trust in the *paper* was rated lowest and, thus, significantly lower compared to the *QR device* ($p = 0.012$), *RFID sticker* ($p = 0.008$), *smartcard* ($p = 0.001$), and the *USB keychain* ($p = 0.019$). We found significant differences in beliefs about whether devices keep the keys secure ($F(4, n/a) = 3.07$, $p = 0.036$). However, post hoc pairwise comparisons did not reveal any significant differences between the conditions after Holm correction.

User Interactions vs. Security Perceptions. As shown in Table 3, SUS scores were positively correlated with trust ($r(63) = 0.58$, $p < 0.001$) and with the belief that the keys are kept secure ($r(63) = 0.41$, $p = 0.011$). Correspondingly, RTLX scores negatively correlated with trust ($r(63) = -0.53$, $p < 0.001$). Thus, prototypes that were perceived as more usable were also rated as more trustworthy and as keeping the keys more secure.

4.3.2 Semi-Structured Interviews.

Security Perceptions. Participants' security perceptions were often shaped by whether and how *access control mechanisms* were implemented ($N = 8$). In particular, participants wished for authentication mechanisms *"so unauthorized access [is not] as much of a problem"* [P3] and were worried about *"the USB flash drive [since] everyone can read [it]"* [P7].

Participants also frequently made *absolute or comparative security judgments* between devices or security implementations ($N = 7$). For instance, they described perceiving data transfer that requires physical contact as more secure. They also perceived single-purpose devices or purely analog methods of data transport as more secure: *"I can imagine taking this sticker with me because it doesn't have any other function, and if you don't know what it does and don't understand what it's for, then it can't be misused."* [P13]; *"I guess paper is the safest option if you take good care of it, because there's absolutely nothing electronic about it."* [P2]

Moreover, our participants described *tangible security* aspects that impacted their security perceptions ($N = 3$). For instance, they suggested adding physical RFID or viewing (privacy) shields to the PTDs. Finally, security perceptions were also impacted by whether participants felt that implemented security measures were *transparent, explainable, or understandable* ($N = 3$): *"If I knew more about how it works, I would feel more secure."* [P9]

Physical Risks. Participants frequently described physical risks to the *confidentiality* of data or devices ($N = 12$). Participants were apprehensive about data being read out from the RFID sticker – and sometimes also the smartcard – in a contactless manner. They also mentioned shoulder surfing, in particular regarding the paper or the QR device: *"It's simply revealing the key. Anyone could easily copy it, photograph it, take it away, or see it."* [P4]

Moreover, participants described risks to the *availability* of the PTDs or the data ($N = 9$). We observed that participants' security perceptions were often rooted in their fear of losing each device. Participants described in detail how they believed the USB keychain, the RFID sticker, and the paper could be lost easily. This fear was related to previous experiences and the belief that they could fall off objects they are attached to: *"I found the USB flash drive to be insecure because I had the experience in the past that this type of USB flash drive with a cord is the most likely to break."* [P10] Similarly, some participants were worried about the *integrity* of the PTDs ($N = 3$). In particular, they were worried that the paper or sticker might be easily destroyed.

Usability. Participants mentioned several usability-related *preferences or positive usability aspects* of the tested PTDs ($N = 10$). In particular, they preferred transporting devices that can be attached or combined with another object they have to carry around, either way, such as the RFID sticker or smartcard: *"the small ones that you can add to the items you have with you anyway, so you don't have to be extra careful about them"* [P9] Correspondingly, providing devices with a physical connection decreased the perceived risk of

	Standard Scales			Security Perceptions					
	SUS	RTLX	HCTS	easily lost	if lost	if access	keys secure	transfer secure	transport easy
Paper	57.03 (13.08)	52.92 (17.51)	2.33 (0.61)	3.62 (1.41)	4.06 (0.85)	3.81 (1.11)	2.56 (1.41)	2.81 (1.33)	4.12 (1.09)
QR device	78.91 (11.03)	23.33 (6.08)	3.30 (0.54)	3.00 (1.15)	3.62 (1.20)	3.75 (1.00)	3.31 (0.87)	3.50 (0.97)	3.38 (1.36)
RFID sticker	91.72 (11.13)	21.15 (9.65)	3.20 (0.53)	3.00 (1.21)	3.56 (0.96)	3.88 (1.02)	3.25 (0.77)	3.31 (0.70)	4.44 (1.03)
Smartcard	86.72 (8.50)	22.03 (4.59)	3.43 (0.53)	2.94 (1.00)	3.69 (1.01)	3.88 (0.96)	3.75 (0.77)	3.88 (0.81)	4.62 (0.50)
USB keyc.	69.53 (17.85)	30.21 (12.40)	3.07 (0.62)	3.56 (1.36)	3.62 (1.20)	4.00 (1.03)	2.94 (1.18)	3.31 (1.14)	4.75 (0.58)

Table 2: Participants' average answers and standard deviations (in parentheses) to standard scales and our additional Likert items. The Likert item ratings can range from 1 (disagree) to 5 (agree).

x	y	r	DoF	95% CI	p
RTLX	HCTS	-0.534	63.0	(-0.69, -0.33)	<0.001
SUS	HCTSl	0.583	63.0	(0.4, 0.72)	<0.001
SUS	keys secure	0.405	63.0	(0.18, 0.59)	0.013

Table 3: Statistically significant repeated measure correlation results for the visions study (p-values Holm corrected).

losing them for our participants. Finally, P2 described a preference for well-established interaction patterns: *"Everything is very user-friendly, with interactions that you are already familiar with, such as inserting a card like at an ATM or a USB flash drive"* [P2]

Our participants also described *usability-related challenges* with PTDs. These challenges were frequently related to data transfer to or from the PTD – in particular, regarding the paper and USB flash drive –, and participants wished for more automation. Another recurring theme was transport-related challenges, with participants not wanting to carry the QR device due to its large size and weight, or the paper, which was also described as too large. However, transporting too small objects was also described as a challenge. Hence, participants suggested using a bigger USB flash drive *"that you don't have to fiddle around with"* [P11] or attaching the RFID sticker *"onto an extra transponder or integrate it into it, so that I still have something physical that I can transport and store more easily"* [P11].

5 Commercial Products Study

In this study, participants tested commercial PTDs selected based on four criteria: They (1) were not much larger than a smartphone and supported changing rather than hard-coded data, (2) represented different form factors (i.e., hard disk drives, USB flash drives, and smartcards), (3) used different authentication factors (knowledge, token, and biometrics), and (4) employed state-of-the-art cryptography (e.g., AES-256-XTS). Table 4 summarizes their properties and authentication factors. Appendix B.1 provides further details.

5.1 Method

As in visions study, two PCs on separate desks represented office and home-office workstations. Participants received written instructions for transferring a secret key to and from each device, including the authentication secrets (different 8-digit PINs). Our questionnaires largely replicated the visions study, but we adapted the additional Likert items in the *condition questionnaire* to capture more detailed security perceptions. Specifically, we assessed perceptions of authentication features and the 'CIA triad' – Confidentiality, Integrity, and Availability, the core values of IT security [10].

5.1.1 Procedure. After collecting consent, an experimenter registered participants' fingerprints for the BioDefender. The remaining procedure closely replicated the visions study: participants completed a *start questionnaire*, performed *key transfer and transport trials* with each device in random order, and completed a *condition questionnaire* after each trial. Finally, we conducted *semi-structured interviews* about participants' assessments and preferences, additionally comparing PTDs to online data exchange and asking about concerns regarding biometric authentication. The study lasted about 90 minutes.

5.1.2 Recruitment & Participants. We again distributed our study invitation through university channels. We recruited 13 participants, of whom 10 identified as male and 3 as female (see Table 5). Our participants were *mean* = 29.38 years old, and most were university graduates ($N = 10$). All participants worked regularly from home (1-2 times per week: $N = 7$, or more often) and resided in Germany. Participants' affinity for technology interaction ($ATI = 3.67$) and security attitudes scores ($SA\text{-}6 = 3.18$) were much higher than averages reported in related work [15, 19, 20]. However, their overall security behavior intentions scores ($SeBIS = 3.35$) were lower than values from related work [15].

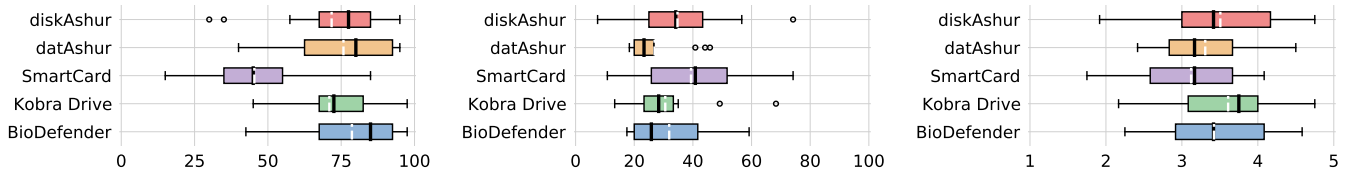
5.2 Results

5.2.1 Condition Questionnaires. We, again, focus on statistically significant findings here and interpret quantitative differences primarily as directional patterns, especially where post-hoc comparisons were not statistically significant. Refer to Appendix B.5 for non-significant findings and the test statistics of post hoc tests. Based on its design, the products study had 80% power to detect paired-samples effects of at least Cohen's $d_z = 0.85$ and repeated-measures correlations of at least $|r| = 0.37$. Smaller effects may have gone undetected.

User Interaction: Usability & Workload. A repeated measures ANOVA yielded significant differences between *SUS scores* of the devices ($F(4, 12) = 6.78$, $p < 0.001$, see Figure 4). The *Thales smartcard* received the lowest usability ratings ($SUS = 45.38(19.47)$) and, thus, was rated significantly worse than the *BioDefender* ($p = 0.034$, $SUS = 78.65(18.02)$), *Kobra Drive* ($p = 0.048$, $SUS = 70.96(15.56)$), *datAshur* ($p = 0.016$, $SUS = 75.77(17.48)$), and the *diskAshur* ($p = 0.034$, $SUS = 71.73(20.27)$). We did not find significant differences between the *task load* resulting from using each device (i.e., RTLX, $\chi^2(4) = 7.58$, $p = 0.108$, Kendall's $W = 0.15$).

	Form Factor			Authentication			Properties
	HDD	USB flash drive	smart-card	secret	bio-metric	token	
iStorage diskAshur Pro 2	X			X			physical keypad
Kobra Drive VS	X		X	X		X	physical keypad
iStorage datAshur Pro		X		X			physical keypad
Kanguru Defender Bio-Elite30		X			X		fingerprint reader
Thales Smartcard ID Prime 930			X	X			reader required

Table 4: The commercially available PTDs we chose combine different form factors and authentication methods.



(a) System Usability (SUS) **(b) Task Load (RTLX)** **(c) Human-Computer Trust (HCTS)**

Figure 4: Standard scale scores comparing the different prototypes evaluated during the product study. Medians are shown through a bold black line and means through a dashed white line.

Gender	Age		ATI	SA6	SeBIS	PTT
10 male	mean = 29.38	**mean**	4.35	6.93	3.35	3.44
3 female	std = 8.26	**std**	0.88	3.16	0.26	0.63

Table 5: Demographics of products study participants.

Security Perceptions: Trust & Own Items . We could not find statistically significant differences between participants' trust in each device ($F(4, 12) = 1.72, p = 0.190$). To assess further security perceptions (see Table 6), we first analyzed internal consistencies among items that target the same objectives. We deemed Cronbach's [11] α values per device acceptable for all item groups considering the small sample size (α_{auth}: 0.87–0.97, α_C: 0.66 – 0.91, α_I: 0.22–0.80, α_A: 0.39–0.55, see Appendix B.4) and thus proceeded to use means for further analyses. Repeated measures ANOVAs revealed significant differences between conditions for *integrity* items ($F(4, 12) = 4.07$, $p = 0.014$). However, post hoc pairwise comparisons did not reveal any significant differences between the products after Holm correction ($p > 0.05$). Nevertheless, we found significant differences between conditions for *availability* ($F(4, 12) = 6.25$, $p = 0.001$). In particular, the *BioDefender* was rated significantly lower in availability than both hard disk drives (i.e., *Kobra Drive* $p = 0.036$ and *diskAshur* $p = 0.024$). Similarly, the *smartcard* received significantly lower availability ratings than the *diskAshur* ($p = 0.004$).

User Interactions vs. Security Perceptions. A repeated measures correlation revealed a positive association between usability (SUS) and trust (HCTS; $r(51) = 0.54$, $p < 0.001$, 95% CI $[0.31, 0.70]$). Thus, devices that participants perceived as more usable were also perceived as more trustworthy.

5.3 Semi-Structured Interviews

Security Perceptions. Our participants' security perceptions were again reflected in their *absolute and relative security judgments* between devices and implemented security features ($N = 12$).

	Standard Scales			Security Perceptions			
	SUS	RTLX	HCTS	authen-tica-tion	confi-dential-ity	integ-rity	avail-ability
BioDefender	78.65 (18.02)	31.92 (15.69)	3.42 (0.84)	4.15 (0.92)	3.88 (0.62)	3.46 (0.79)	2.29 (0.80)
Kobra Drive	70.96 (15.56)	30.58 (14.59)	3.61 (0.72)	4.04 (0.88)	3.76 (0.88)	3.38 (0.76)	3.08 (0.67)
Smartcard	45.38 (19.47)	39.36 (17.61)	3.12 (0.73)	3.88 (1.18)	3.23 (0.80)	2.59 (0.82)	2.40 (0.62)
datAshur	75.77 (17.48)	26.92 (9.86)	3.31 (0.71)	3.62 (1.08)	3.53 (1.00)	3.18 (0.95)	2.75 (0.65)
diskAshur	71.73 (20.27)	34.74 (18.23)	3.51 (0.92)	3.88 (0.96)	3.72 (0.92)	3.28 (1.00)	3.10 (0.73)

Table 6: Average standard scores and perceived security of the compared products (std in ()). Perceived security is rated from 1=disagree to 5=agree.

Participants frequently compared biometric authentication with password-based mechanisms. However, opinions varied largely, as some participants perceived biometric methods as more secure than passwords and others perceived biometrics as less secure. Smartcards were also sometimes perceived as comparatively insecure.

Participants also described reasons for believing that *physical data transport is more secure compared to online data exchange* ($N = 10$). They felt in control when transporting data physically, and physical transport was perceived as more isolated. They expressed less trust in online systems, framed online environments as generally insecure, and were worried about online eavesdropping. However, one participant felt that online data exchange would be more secure, because they assumed fewer points of failure due to personal previous experiences: *"I feel that there is less that can go wrong"* [P1]. Security perceptions were also often guided by *access control mechanisms* ($N = 8$). In particular, multi-factor authentication was perceived as very secure.

Participants also emphasized strong or complex passwords and noted that the type of authentication mechanism mattered to them. Moreover, they discussed the impact of *transparency, explainability, and understandability* of security features ($N = 4$). Some participants expressed uncertainty about how the PTDs functioned, and that not knowing these details affected their security perception. Others referred to the use of common encryption methods or open-source approaches as positively influencing their perception. They also mentioned certifications by independent authorities or indicated that the PTD should not show that it carries secrets.

Finally, some participants again reflected on *tangible security* aspects ($N = 2$). For instance, they described that the appearance of the PTD and, in particular, the *"physical PIN entry system [feels] more secure than anything else"* [P13].

Physical Risks. Participants of the products study focused strongly on *availability* ($N = 13$). They described losing the PTD, feeling that small devices have an elevated risk, and also mentioned theft. Some participants also worried about the battery being empty, the availability of the token, or forgetting the password. Nevertheless, participants of the products study also described risks regarding the *confidentiality* ($N = 10$) and *integrity* ($N = 10$) of the tested devices of the transported data. Participants frequently mentioned physical damage, in particular in regard to the smartcard: *"it's so fragile"* [P11]. Participants also worried about smartcards or USB flash drives being hacked easily or mentioned observation attacks in regard to physical PIN entry: *"I believe it can be read with any generic smartcard reader"* [P6].

Usability. Participants of the products study also described *usability preferences or advantages* ($N = 7$). They especially acknowledged the ease of use of fingerprint-based authentication. They also noted that while two-factor authentication increases security perceptions, it also constitutes a barrier and stressed that such mechanisms need to remain usable. One participant mentioned that preferences depend on the usage context, and another described that familiarity played a role. However, participants also described a variety of *usability-related challenges* ($N = 10$). In particular, they described issues related to physical interaction, such as having to apply too much force when pressing buttons or a USB cable that was too short and mentioned the weight of the Kobra drive.

6 Discussion

We contrast our findings with related work and our threat analysis (Section 3.1.2) to answer our RQs, discuss participants' risk awareness, and potential misconceptions. Based on this, we derive key takeaways for researchers, device manufacturers, and organizations deploying PTDs to mitigate risks by design.

6.1 Impact of User Interactions & Form Factors

RQ1 asked *how form factors of PTDs and interactions with them shape security perceptions.* We discuss corresponding findings below.

6.1.1 Usability and Security Perceptions Align. Confirming related work on physical authentication devices [13], our findings show that more usable PTDs are also trusted more, *emphasizing that user interactions indeed shape security perceptions of PTDs.* However, it is important to note that the user interaction consists of a combination of actions users must perform to start the data transfer and interactions resulting from security features (e.g., authentication). The smartcards used in both studies illustrate this, as their usability was rated much higher in the visions study than in the products study. In the latter, users had to enter a PIN via the PC's keyboard before reading the data. This software-based PIN entry was perceived as less usable than other devices' physical PIN entry.

> **Takeaway:** Good usability correlates with increased security perceptions. In order to design for usability, the entire user interaction must be considered and be as simple and as tangible as possible. This also includes user interaction steps performed inside software, which we suggest reducing to a minimum.

6.1.2 Impact of Desired Form Factors on Perceived and Actual Security Threats. We also observed that *losing a PTD was the most prominently considered security risk*, strongly shaping our participants' form-factor preferences. Consistent with related work, large and heavy devices were considered bothersome [38], while small devices were perceived as easy to lose, motivating attachment to routinely carried objects (e.g., to keychains or wallets).

Such attachments may also result in the alignment of desired security behavior (e.g., not leaving PTDs in public spaces unattended) with existing "custody habits". By integrating the PTD into routines where users already act mindfully, such as protecting their keychain or smartphones, one can (a) reduce the objective risk of physical loss or theft and (b) alleviate subjective anxieties (e.g., the fear of losing the PTD). Moreover, while participants did not specifically mention tampering, such preferred small and attached form factors would be also frequently transported relatively closely to the users' bodies, potentially reducing the propensity for Evil Maid attack. However, such form factors could also result in users transporting the PTD even when they do not need it and potentially attaching multiple devices to the same object. This could severely aggravate the impact of denial-of-service threats.

> **Takeaway:** For users, the optimal device size appears to correspond to a smart card. Moreover, physical attachments to objects that users routinely carry reduce perceived transportation effort and the risk of loss. These attachments may additionally trigger established desirable protective behaviors. However, they may also aggravate the consequences of Denial of Service attacks.

6.1.3 Reduce Perceived Fragility. As suggested in related work [36], we confirmed that materials and shapes of the PTD influence perceived security. Devices that are perceived as too fragile (i.e., made of paper or thin plastics) trigger fears of destruction and thus limitations in availability and/or integrity. Moreover, we found that the connection to other objects must appear sturdy and be permanently and reliably guaranteed, as even singular negative experiences influence users' perception of security. Nevertheless such anxieties may in turn lead to more protective behavior, reducing actual security risks. Ergonomics of the shape of the PTD are also important, as devices or interaction mechanisms that are too small or hard to actuate were perceived as fiddly and difficult to interact with.

Takeaway: Material- and shape-related design choices impacted security perceptions, as users are strongly guided by integrity- and availability-related fears. Hence, to increase perceived security the materials and shapes of a PTD must be sufficiently sturdy so that users do not fear damaging it, while also being comfortable to manipulate and ergonomic.

6.2 Implemented Security Measures

RQ2 inquired *how manifestations of security measures (i.e., connectivity and authentication mechanisms) impact users' security perceptions of commercial PTDs.*

6.2.1 Wireless is Perceived as Insecure. Although the RFID sticker and the smartcard received high usability ratings in the visions study, participants perceived wireless data transfer as insecure. In particular, they were worried about shoulder surfing and felt that these PTDs could be read out by anybody nearby. This preference for physical connection was also reflected in the fact that participants described the smartcard as more secure than the RFID sticker, since they believed that the transmission range of the smartcard is smaller. This pointed out existing misconceptions, as both devices use RFID technology. Thus, physical interaction requirements, such as inserting a device, may increase perceived control without necessarily providing the protection users infer from them.

Takeaway: Although wireless data transmission is very usable, it is also perceived as much less secure. We, therefore, recommend implementing wired connections for data transfer or at least insert-to-read-out technologies to increase users' sense of security. More generally, connectivity mechanisms should make actual access boundaries visible and understandable.

6.2.2 Physical Isolation and Interaction are Reassuring. Participants also perceived physical data exchange as especially secure when it occurs entirely offline. Hence, PTDs should ideally never be connected to the internet, even if the stored data is never transmitted, as our findings indicate a general mistrust of online environments. For example, maintenance should also require no internet connection to maintain users' perception of complete isolation. Similarly, participants expressed a preference for physical PIN entry and for physically isolating measures, such as RFID or privacy shields. These measures leave users feeling in control of data transport and security, which might impact their perceived self-efficacy. Research on tangible privacy in smart home environments suggests that physical controls, such as buttons, covers, and switches, increase users' feeling of control and thus reduce security-related concerns [2, 16]. These findings highlight that our participants were largely aware of information disclosure-related threats.

Takeaway: To maximize perceived security, PTDs should be as digitally and physically isolated as possible, meaning that they should not require access to the internet and incorporate physical isolation reassurances, such as shields for access points. This can be combined with tangible user input means to increase users' perception of being in control.

6.3 Security Perceptions vs. Actual Threats

Participants in both user studies reported that their security perceptions were limited by their understanding of implemented security measures. We also observed misconceptions. For instance, they assumed different security levels for RFID-based devices based on their form and interaction, and were unsure if biometric authentication is more secure than an 8-digit PIN. This may result in users unknowingly behaving in an insecure manner when using a PTD [39, 42, 47]. We thus reflect on our participants' risk awareness.

Participants identified several relevant threats, particularly denial of services related, such as loss, theft, and physical damage. They also considered information disclosure-related risks, but rarely considered deliberate tampering or spoofing. For instance, only one of our participants mentioned that any of the PTDs – USB keychain – could be easily replaced by a similar device. Moreover, PTDs may be especially prone to repudiation, as users may not necessarily feel comfortable with the personal responsibility resulting from using a physical device [38]. Nevertheless, our participants described the resulting feeling of being in control of the data exchange positively, which suggests that while they are aware of the heightened responsibility, they do not appear to be intimidated by it.

Takeaway: While technical, interactional, and physical design properties can positively influence security perceptions, our results also highlight a broad diversity of security perceptions and (mis-)conceptions. Consequently, we recommend that designers and organizations investigate the security perceptions of their targeted end-users regarding PTDs and integrate these findings into their corresponding decision-making processes.

6.4 Open Questions for Future Research

Authentication and Broader Security Perceptions. The contrasting smartcard results across our studies suggest that authentication implementations may affect usability and broader security perceptions differently. While software-based PIN entry (only required during the products study) coincided with lower usability and broader security perceptions, authentication-specific ratings remained comparable across devices. Future research should therefore investigate how different authentication mechanisms in PTDs simultaneously shape perceived usability and broader security perceptions.

Applicability Across Personal Security Attitudes and Cultural Contexts. Our participants' security perceptions were often influenced by their prior experiences with PTDs and their understanding of the implemented security measures. This suggests that users with different security attitudes or (cultural) backgrounds may form security perceptions that are impacted differently by design and implementation features of PTD. This open question is particularly interesting as related work has found a correlation between security attitudes of individuals or their previous experiences and their preference for physical (i.e., tangible) privacy mechanisms [15].

7 Conclusion

Physical data transport remains important for especially critical information. However, the security of these devices often relies

on users physically safeguarding them. Since misconceptions regarding cybersecurity are widespread among both normal users and experts, we explored how design cues, interaction patterns, and implemented security features shape the user's security perceptions of physical transport devices (PTDs). We conducted two complementary mixed-methods studies that involved participants performing a complete data transfer scenario with ten different devices. Based on our findings, we derived key takeaways for the design and adoption of devices and identified related misconceptions. Our work, therefore, provides a foundation for physically explainable security by design.

Acknowledgments

We would like to thank our study participants for their efforts and input. This project has been funded by the European Union – NextGeneration EU and the dtec.bw – Center for Digitization and Technology Research of the Bundeswehr (Project MuQuaNet).

References

[1] Anne Adams and Martina Angela Sasse. 1999. Users Are Not the Enemy. *Commun. ACM* 42, 12 (dec 1999), 40–46. doi:10.1145/322796.322806

[2] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. 2020. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW2 (Oct. 2020), 116:1–116:28. doi:10.1145/3415187

[3] Omer Akgul, Wei Bai, Shruti Das, and Michelle L. Mazurek. 2021. Evaluating In-Workflow Messages for Improving Mental Models of End-to-End Encryption. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 447–464. https://www.usenix.org/conference/usenixsecurity21/presentation/akgul

[4] Wei Bai, Michael Pearson, Patrick Gage Kelley, and Michelle L. Mazurek. 2020. Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 210–219. doi:10.1109/EuroSPW51379.2020.00036

[5] Khadija Baig, Elisa Kazan, Kalpana Hundlani, Sana Maqsood, and Sonia Chiasson. 2021. Replication: Effects of Media on the Mental Models of Technical Users. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, 119–138. https://www.usenix.org/conference/soups2021/presentation/baig

[6] Jonathan Z. Bakdash and Laura R. Marusich. 2017. Repeated Measures Correlation. *Frontiers in Psychology* Volume 8 - 2017 (2017). doi:10.3389/fpsyg.2017.00456

[7] Odette Beris, Adam Beautement, and M. Angela Sasse. 2015. Employee Rule Breakers, Excuse Makers and Security Champions: Mapping the risk perceptions and emotions that drive security behaviors. In *Proceedings of the 2015 New Security Paradigms Workshop* (Twente, Netherlands) *(NSPW '15)*. Association for Computing Machinery, New York, NY, USA, 73–84. doi:10.1145/2841113.2841119

[8] John Brooke. 1996. *SUS – a quick and dirty usability scale.* Taylor & Francis, 189–194.

[9] L Jean Camp. 2009. Mental models of privacy and security. *IEEE Technology and society magazine* 28, 3 (2009), 37–46.

[10] Kodi A. Cochran. 2024. *The CIA Triad: Safeguarding Data in the Digital Realm.* Apress, Berkeley, CA, 17–32. doi:10.1007/979-8-8688-0432-8_2

[11] Lee J Cronbach and Paul E Meehl. 1955. Construct validity in psychological tests. *Psychological bulletin* 52, 4 (1955), 281.

[12] Rikke Friis Dam and Teo Yu Siang. 2025. https://www.interaction-design.org/literature/article/how-to-select-the-best-idea-by-the-end-of-an-ideation-session?srsltid=AfmBOoprg06228VikfEYus7H0ObAW7DppImFLQoOWIQlB2vumhhhkY3L last accessed February 4, 2026.

[13] Emiliano De Cristofaro, Honglu Du, Julien Freudiger, and Greg Norcie. 2013. A comparative usability study of two-factor authentication. *arXiv preprint arXiv:1309.5344* (2013).

[14] Sergej Dechand, Alena Naiakshina, Anastasia Danilova, and Matthew Smith. 2019. In Encryption We Don't Trust: The Effect of End-to-End Encryption to the Masses on User Perception. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. 401–415. doi:10.1109/EuroSP.2019.00037

[15] Sarah Delgado Rodriguez, Priyasha Chatterjee, Anh Dao Phuong, Florian Alt, and Karola Marky. 2024. Do You Need to Touch? Exploring Correlations between Personal Attributes and Preferences for Tangible Privacy Mechanisms. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 981, 23 pages. doi:10.1145/3613904.3642863

[16] Sarah Delgado Rodriguez, Maximiliane Windl, Florian Alt, and Karola Marky. 2025. The TaPSI Research Framework - A Systematization of Knowledge on Tangible Privacy and Security Interfaces. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 923, 28 pages. doi:10.1145/3706598.3713968

[17] Verena Distler, Tamara Gutfleisch, Carine Lallemand, Gabriele Lenzini, and Vincent Koenig. 2022. Complex, but in a good way? How to represent encryption to non-experts through text and visuals – Evidence from expert co-creation and a vignette experiment. *Computers in Human Behavior Reports* 5 (2022), 100161. doi:10.1016/j.chbr.2021.100161

[18] Serge Egelman and Eyal Peer. 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 2873–2882. doi:10.1145/2702123.2702249

[19] Cori Faklaris, Laura Dabbish, and Jason Hong. 2019. A Self-Report Measure of End-User Security Attitudes (SA-6). In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Berkeley, CA, Santa Clara, CA, USA. doi:10.13140/RG.2.2.29840.05125/3

[20] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. 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 (2019), 456–467. doi:10.1080/10447318.2018.1456150

[21] Milton Friedman. 1939. A Correction. *J. Amer. Statist. Assoc.* 34, 205 (1939), 109–109. doi:10.1080/01621459.1939.10502372

[22] Kelsey R. Fulton, Rebecca Gelles, Alexandra McKay, Yasmin Abdi, Richard Roberts, and Michelle L. Mazurek. 2019. The Effect of Entertainment Media on Mental Models of Computer Security. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 79–95. https://www.usenix.org/conference/soups2019/presentation/fulton

[23] Samuel W Greenhouse and Seymour Geisser. 1959. On methods in the analysis of profile data. *Psychometrika* 24, 2 (1959), 95–112.

[24] Federico Griscioli and Maurizio Pizzonia. 2016. Securing promiscuous use of untrusted USB thumb drives in Industrial Control Systems. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. 477–484. doi:10.1109/PST.2016.7907002

[25] Siddharth Gulati, Sonia Sousa, and David Lamas. 2018. Modelling trust in human-like technologies. In *Proceedings of the 9th Indian conference on human computer interaction*. 1–10. doi:10.1145/3297121.3297124

[26] Siddharth Gulati, Sonia Sousa, and David Lamas. 2019. Design, development and evaluation of a human-computer trust scale. *Behaviour & Information Technology* 38, 10 (2019), 1004–1015. doi:10.1080/0144929X.2019.1656779

[27] Sandra G. Hart and Lowell E. Staveland. 1988. Development of NASA-TLX (Task Load Index): Results of Empirical and Theoretical Research. In *Human Mental Workload*, Peter A. Hancock and Najmedin Meshkati (Eds.). Advances in Psychology, Vol. 52. North-Holland, 139–183. doi:10.1016/S0166-4115(08)62386-9

[28] Sture Holm. 1979. A simple sequentially rejective multiple test procedure. *Scandinavian journal of statistics* (1979), 65–70.

[29] Jongkil Jay Jeong, Syed Wajid Ali Shah, Ashish Nanda, Robin Doss, Mohammad Nosouhi, and Jeb Webb. 2024. User Characteristics and Their Impact on the Perceived Usable Security of Physical Authentication Devices. *IEEE Transactions on Human-Machine Systems* 54, 5 (2024), 554–564. doi:10.1109/THMS.2024.3421538

[30] Michaela Kauer, Sebastian Günther, Daniel Storck, and Melanie Volkamer. 2013. A Comparison of American and German Folk Models of Home Computer Security. In *Human Aspects of Information Security, Privacy, and Trust*, Louis Marinos and Ioannis Askoxylakis (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 100–109. doi:10.1007/978-3-642-39345-7_11

[31] Rafiullah Khan, Kieran McLaughlin, David Laverty, and Sakir Sezer. 2017. STRIDE-based threat modeling for cyber-physical systems. In *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*. 1–6. doi:10.1109/ISGTEurope.2017.8260283

[32] Loren Kohnfelder and Praerit Garg. 1999. The threats to our products. *Microsoft Interface, Microsoft Corporation* 33 (1999), 1–8.

[33] Hongyi Lu, Yechang Wu, Shuqing Li, You Lin, Chaozu Zhang, and Fengwei Zhang. 2021. BADUSB-C: Revisiting BadUSB with Type-C. In *2021 IEEE Security and Privacy Workshops (SPW)*. 327–338. doi:10.1109/SPW53761.2021.00053

[34] Karola Marky, Martin Schmitz, Verena Zimmermann, Martin Herbers, Kai Kunze, and Max Mühlhäuser. 2020. 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)*. Association for Computing Machinery, New York, NY, USA, 1–12. doi:10.1145/3313831.3376189

[35] Harrison McKnight, Michelle Carter, and Paul Clay. 2009. Trust in technology: Development of a set of constructs and measures. (2009). http://aisel.aisnet.org/digit2009/10

[36] Ashish Nanda, Jongkil Jay Jeong, Syed Wajid Ali Shah, Mohammad Nosouhi, and Robin Doss. 2024. Examining usable security features and user perceptions of Physical Authentication Devices. *Computers & Security* 139 (April 2024), 103664.

doi:10.1016/j.cose.2023.103664
[37] National Institute of Standards and Technology. 2025. *Reducing the Cybersecurity Risks of Portable Storage Media in OT Environments.* Special Publication (NIST SP) 1334. National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA. doi:10.6028/NIST.SP.1334
[38] Jeunese Payne, Graeme Jenkinson, Frank Stajano, M Angela Sasse, and Max Spencer. 2016. Responsibility and tangible security: Towards a theory of user acceptance of security tokens. *arXiv preprint arXiv:1605.03478* (2016). https://doi.org/10.48550/arXiv.1605.03478
[39] Svenja Schroeder, Markus Huber, David Wind, and Christoph Rottermanner. 2016. When SIGNAL hits the Fan: On the Usability and Security of State-of-the-Art Secure Mobile Messaging. In *Proceedings 1st European Workshop on Usable Security.* Internet Society, Darmstadt, Germany. doi:10.14722/eurousec.2016.23012
[40] S. S. Shapiro and M. B. Wilk. 1965. An analysis of variance test for normality (complete samples)†. *Biometrika* 52, 3-4 (12 1965), 591–611. doi:10.1093/biomet/52.3-4.591
[41] Luigi Sportiello. 2019. "Internet of Smart Cards": A pocket attacks scenario. *International Journal of Critical Infrastructure Protection* 26 (2019), 100302. doi:10.1016/j.ijcip.2019.05.005
[42] Christian Stransky, Oliver Wiese, Volker Roth, Yasemin Acar, and Sascha Fahl. 2022. 27 Years and 81 Million Opportunities Later: Investigating the Use of Email Encryption for an Entire University. In *2022 IEEE Symposium on Security and Privacy (SP).* 860–875. doi:10.1109/SP46214.2022.9833755
[43] Matthew Tischer, Zakir Durumeric, Sam Foster, Sunny Duan, Alec Mori, Elie Bursztein, and Michael Bailey. 2016. Users Really Do Plug in USB Drives They Find. In *2016 IEEE Symposium on Security and Privacy (SP).* 306–319. doi:10.1109/SP.2016.26
[44] Mark Turner, Martin Schmitz, Morgan Masichi Bierey, Mohamed Khamis, and Karola Marky. 2023. Tangible 2FA – An In-the-Wild Investigation of User-Defined Tangibles for Two-Factor Authentication. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023).* USENIX Association, Anaheim, CA, 245–261. https://www.usenix.org/conference/soups2023/presentation/turner
[45] Luca Viganò and Daniele Magazzeni. 2020. Explainable Security. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).* 293–300. doi:10.1109/EuroSPW51379.2020.00045
[46] Melanie Volkamer and Karen Renaud. 2013. *Mental Models – General Introduction and Review of Their Application to Human-Centred Security.* Springer Berlin Heidelberg, Berlin, Heidelberg, 255–280. doi:10.1007/978-3-642-42001-6_18
[47] Rick Wash. 2010. Folk Models of Home Computer Security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (Redmond, Washington, USA) *(SOUPS '10).* Association for Computing Machinery, New York, NY, USA, Article 11, 16 pages. doi:10.1145/1837110.1837125
[48] Rick Wash and Emilee Rader. 2015. Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015).* USENIX Association, Ottawa, 309–325. https://www.usenix.org/conference/soups2015/proceedings/presentation/wash
[49] Frank Wilcoxon. 1945. Individual comparisons by ranking methods. *Biometrics bulletin* 1, 6 (1945), 80–83.
[50] Justin Wu and Daniel Zappala. 2018. When is a Tree Really a Truck? Exploring Mental Models of Encryption. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018).* USENIX Association, Baltimore, MD, 395–409. https://www.usenix.org/conference/soups2018/presentation/wu

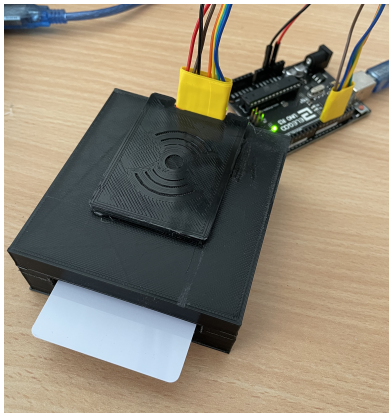
This appendix provides additional information on our study design and findings. In addition, we provide supplementary material (incl. the study guides) in a separate folder.

A Visions Study

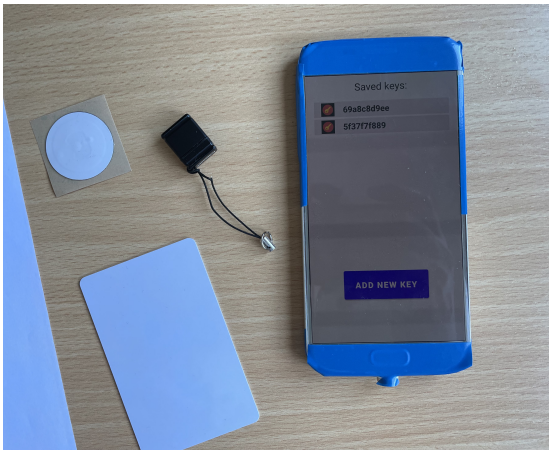
A.1 Focus Group Questions

(1) What challenges or problems does the hardware device have to solve?
(2) How could the key be transferred onto the device?
(3) How would you transport such a hardware device?
(4) How could the key be transferred onto the PC?
(5) How could such a hardware device look?

A.2 Self-Built Reader and Device Prototypes



(a) The smartcard/RFID reader contains an Arduino Uno R3 microcontroller and an MFRC522 RFID breakout.



(b) Prototypical devices used in the visions study.

Figure 5: Photos of the self-built smartcard/RFID reader and the devices we used for our visions study.

A.3 Additional Likert-Items

- I believe this prototype could get easily lost
- I believe this prototype is easily transportable
- I am aware of the consequences of losing the prototype.
- I am aware of the consequences if another person gains access to the prototype.
- I believe the prototype is keeping the keys secure
- I feel the transmission of the keys to and from the prototype is secure.

A.4 Additional Statistical Results

item	test	result
easily lost	RM-ANOVA	$F(4, 15) = 1.24$, $p = .305$
if lost	RM-ANOVA	$F(4, 15) = 0.90$, $p = .440$
if access	RM-ANOVA	$F(4, 15) = 0.75$, $p = .518$
keys secure	RM-ANOVA	$F(4, 15) = 3.07$, $p = .036$
transfer secure	RM-ANOVA	$F(4, 15) = 2.40$, $p = .086$

Table 7: Non-significant results of comparative tests in the visions study.

A	B	T	p
Paper	QR device	-4.99	0.001
Paper	RFID sticker	-10.67	0.000
Paper	Smartcard	-9.95	0.000
QR device	RFID sticker	-3.80	0.010
RFID sticker	USB keyc.	4.04	0.007
Smartcard	USB keyc.	3.56	0.014

(a) SUS, T-Test

A	B	W	p
Paper	QR device	0.0	0.000
Paper	RFID sticker	0.0	0.004
Paper	Smartcard	0.0	0.000
Paper	USB keyc.	4.0	0.007

(b) RTLX, Wilcoxon Test

A	B	T	p
Paper	QR device	-3.88	0.012
Paper	RFID sticker	-4.11	0.008
Paper	Smartcard	-5.40	0.001
Paper	USB keyc.	-3.58	0.019

(c) HCTS, T-Test

Table 8: Post Hoc tests results with test statistics for significant differences between conditions in the visions study.

x	y	r	p	DoF	95% CI
transport easy	easily lost	-0.161	1.00	63	(-0.39, 0.09)
transport easy	HCTS	0.065	1.00	63	(-0.18, 0.30)
transport easy	if access	0.082	1.00	63	(-0.17, 0.32)
transport easy	keys secure	0.019	1.00	63	(-0.23, 0.26)
transport easy	transfer secure	-0.059	1.00	63	(-0.30, 0.19)
transport easy	if lost	-0.058	1.00	63	(-0.30, 0.19)
RTLX	easily lost	0.026	1.00	63	(-0.22, 0.27)
RTLX	if access	-0.053	1.00	63	(-0.29, 0.19)
RTLX	keys secure	-0.263	0.482	63	(-0.48, -0.02)
RTLX	transfer secure	-0.162	1.00	63	(-0.39, 0.09)
RTLX	if lost	0.032	1.00	63	(-0.21, 0.27)
SUS	easily lost	-0.288	0.30	63	(-0.50, -0.05)
SUS	if access	-0.058	1.00	63	(-0.30, 0.19)
SUS	transfer secure	0.261	0.482	63	(0.02, 0.47)
SUS	if lost	-0.021	1.00	63	(-0.26, 0.22)

Table 9: Non-significant (i.e., Holm-corrected $p >= 0.05$) repeated measures correlation results from the visions study.

B Products Study

B.1 Descriptions of the Commercial Products

iStorage diskAshur Pro 2: This hard drive (256GB) implements user authentication via a 7-15 digit PIN that has to be entered using an integrated keypad. Whenever the device is disconnected, it auto-locks. The device has NCSC CPA, NLNCSA BSPA, and FIPS 140-2 Level 3 certifications. It is approved for use in the NATO-Restricted domain.

Kobra Drive VS: This hard drive (1TB) uses a two-factor authentication mechanism: a smartcard and a numeric PIN that has to be entered using an integrated keypad are required to unlock the device. Lock-out and time-out functions are also available. The device is approved by the BSI for the VS-NfD level, as well as for EU-Restricted and NATO-Restricted data.

iStorage datAshur Pro: This USB flash drive had a capacity of 64 GB. Users need to enter a 7-15 digit PIN using the integrated keypad to authenticate. The device contains a rechargeable battery that enables PIN entry before it is inserted into the USB port. The device has NLNCSA DEP-V and FIPS 140-2 Level 3 certifications. It is approved for use in the NATO-Restricted domain.

Kanguru Defender Bio-Elite30: The Kanguru Defender Bio-Elite30 is a USB flash drive (16GB) that uses AES-XTS encryption with a 256-bit key. The device is the smallest in our study and incorporates a biometric fingerprint scanner. Due to the biometric authentication, the device needs to be set up with the software from the manufacturer. It has no independent certification, but the manufacturer claims to comply with the industry security standards HIPAA, Sarbanes-Oxley, GLBA, and GDPR.

Thales Smartcard ID Prime 930: The smartcard applies the ID-1 format. It can apply AES with key lengths of 128, 192, or 256 bits. It has 400 kB of flash memory, of which 78 kB can be used to store data. An additional reader is required to use the smartcard (we used an HID Omnikey 3121 reader), and users must enter an alphanumeric password of 4-64 characters. The ID Prime 930 cards are certified FIPS 140-2 Level 2. The smartcard is approved for use by U.S. federal employees.

B.2 Additional Likert Items

- I feel confident that the data stored on the device cannot be accessed by unauthorized persons. (Auth)
- I think that the authentication mechanism used by the device is secure. (Auth)
- I think the data on the device cannot be manipulated/changed without authorized access. (I)
- I think the device can be easily faked and/or replaced. (I)
- I feel confident that I could distinguish between the real device and a fake. (I)
- I think the device is prone to hacking. (C)
- I feel confident that the data on this device is secure, even in case it is lost or stolen. (C)
- I think the data on this device cannot be accessed via contactless methods (e.g., cloning). (C)
- I think the data on this device is stored securely. (C)
- I think there is no risk when transmitting data to the device. (C)
- I fear for my personal data stored on/used by the device. (C)
- I think the device can be easily lost. (A)
- I think the device can be easily stolen. (A)
- There is a high risk of damaging the device. (A)
- The device is difficult to replace. (A)

B.3 Answers to all Additional Likert Items

(*) denotes reverse-coded items in the following Tables (i.e., 1 = agree and 5 = disagree instead of 1 = disagree and 5 = agree) and the listed values are means and standard deviation in parentheses.

	(Auth) no access by unautho-rised	(Auth) authenti-cation mechanism secure	(I) distin-guish real device and fake	(I) data cannot be manipu-lated	(I) easily faked/ replaced*
BioDefender	4.31 (0.75)	4.00 (1.15)	2.77 (1.48)	4.00 (1.00)	3.62 (1.26)
Kobra Drive	4.08 (0.86)	4.00 (1.00)	3.00 (1.15)	3.69 (1.03)	3.46 (1.05)
Smartcard	4.00 (1.15)	3.77 (1.24)	1.85 (0.80)	3.08 (1.26)	2.85 (1.28)
datAshur	3.62 (1.19)	3.62 (1.04)	2.69 (1.32)	3.69 (1.03)	3.15 (0.99)
diskAshur	3.85 (0.99)	3.92 (1.04)	3.00 (1.22)	3.62 (1.04)	3.23 (1.48)

	(C) fear for my data*	(C) is secure, if lost or stolen	(C) no contact-less access	(C) stored se-curely	(C) prone to hack-ing*	(C) no risk when trans-mitting
BioDefender	4.08 (0.64)	3.92 (0.95)	3.92 (1.12)	4.15 (1.07)	3.54 (1.05)	3.69 (1.18)
Kobra Drive	3.77 (1.09)	4.00 (1.15)	3.77 (1.17)	3.77 (1.01)	3.62 (1.04)	3.62 (1.19)
Smartcard	3.85 (1.07)	3.38 (1.12)	2.38 (1.26)	3.62 (0.96)	2.92 (0.76)	3.23 (1.30)
datAshur	3.85 (1.14)	3.38 (1.12)	3.85 (1.34)	3.69 (1.03)	3.23 (1.17)	3.15 (1.34)
diskAshur	3.77 (1.09)	3.69 (1.11)	3.85 (1.28)	4.00 (0.91)	3.46 (1.20)	3.54 (1.33)

	(A) easily lost*	(A) easily stolen*	(A) difficult to replace*	(A) risk of damaging*
BioDefender	1.38 (0.87)	2.23 (1.48)	2.69 (1.25)	2.85 (1.57)
Kobra Drive	3.15 (1.14)	3.31 (1.25)	2.38 (1.19)	3.46 (0.88)
Smartcard	2.00 (0.82)	2.15 (0.80)	3.46 (1.20)	2.00 (0.91)
datAshur	1.92 (0.86)	2.31 (1.03)	3.38 (1.19)	3.38 (1.26)
diskAshur	3.54 (0.97)	2.85 (1.07)	2.69 (1.11)	3.31 (1.32)

B.4 Internal Consistency of Additional Likert Item Answers

device	Cronbach's alpha Auth	C	I	A
Kobra Drive	0.867	0.877	0.479	0.399
iStorage diskAshur	0.889	0.884	0.701	0.551
iStorage datAshur	0.929	0.910	0.802	0.393
BioDefender	0.883	0.664	0.217	0.430
Thales Smartcard	0.965	0.821	0.540	0.550

B.5 Additional Statistical Results

item	test	result
HCTS	RM-ANOVA	$F(4, 12) = 1.72$, $p = .190$
RTLX	Friedman	$\chi^2(4) = 7.58$; $p = .108$; Kendall's $W = 0.15$
Auth	RM-ANOVA	$F(4, 12) = 0.75$, $p = .523$
C	RM-ANOVA	$F(4, 12) = 2.68$, $p = .071$
I	RM-ANOVA	$F(4, 12) = 4.07$, $p = .014$

Table 10: Non-significant results of comparative tests in the products study.

A	B	T	p
BioDefender	Smartcard	3.527	0.034
Kobra Drive	Smartcard	3.260	0.048
Smartcard	datAshur	-4.052	0.016
Smartcard	diskAshur	-3.575	0.034

(a) SUS, T-Test

A	B	T	p
BioDefender	Kobra Drive	-3.486	0.036
BioDefender	diskAshur	-3.774	0.024
Smartcard	diskAshur	-4.782	0.004

(b) Availability (A), T-Test

Table 11: Post Hoc tests results with test statistics for significant differences between conditions in the products study.

x	y	r	p	DoF	95% CI
RTLX	A	-0.146	1.00	51	(-0.40, 0.13)
RTLX	Auth	0.021	1.00	51	(-0.25, 0.29)
RTLX	C	-0.184	1.00	51	(-0.43, 0.09)
RTLX	I	-0.085	1.00	51	(-0.35, 0.19)
RTLX	HCTS	-0.253	0.473	51	(-0.49, 0.02)
SUS	A	0.163	1.00	51	(-0.11, 0.41)
SUS	Auth	0.092	1.00	51	(-0.18, 0.35)
SUS	C	0.35	0.092	51	(0.09, 0.57)
SUS	I	0.298	0.241	51	(0.03, 0.53)

Table 12: Non-significant (i.e., Holm-corrected $p >= 0.05$) repeated measures correlation results from the products study.

C Codebook

Table 13: Final codebook for the product and vision study. (*) denotes a container for sub-codes and is not used during coding.

Code	Description	Visions	Products
Security Perceptions (*)	Perceived security of devices, mechanisms, and contexts.	–	–
Tangible Security	Security attributed to physical characteristics (e.g., physical PIN, external entry device, form factor).	3	2
Absolute Security Judgments & Comparisons	Direct comparisons or absolute judgments regarding which device or mechanism is more or less secure.	7	12
Transparency & Understandability	Perceived transparency, explainability, certification, or understanding of how security works.	3	4
Access Control Mechanisms	Structural and technical access protection mechanisms (e.g., strong passwords, MFA, layered authentication).	8	8
Online vs Physical (*)	Perceived differences between online/digital and physical security contexts.	–	–
Physical More Secure	Statements expressing that transporting data on physical devices is perceived as more secure.	0	10
Online More Secure	Statements expressing that transporting data online/digital is perceived as more secure.	0	1
Physical Risks (*)	Perceived physical security risks categorized along CIA dimensions.	–	–
Integrity	Risks related to manipulation or alteration of data or devices.	3	10
Confidentiality	Risks related to unauthorized access or data disclosure.	12	10
Availability	Risks related to loss, theft, malfunction, or unavailability of devices or data.	9	13
Usability (*)	Usability-related perceptions and evaluations of devices or mechanisms.	–	–
Preferences & Benefits	Statements expressing advantages, preferences, or positive usability aspects.	10	7
Challenges	Usability challenges, difficulties, or negative experiences.	15	10