Appendix A.
Tasks

Table 1. LAB STUDY TASKS.

No.	Task
1	Log in to the account portal (1st tab in the Safari browser) using the provided username and one-time password. Set an appropriate password and complete the guided tour at your own pace.
2	According to the university's IT security policy, multi-factor authentication should be activated for your account. Add the MFA method [METHOD].
3	You now want to test this MFA method. Log in to another university website using the MacBook: 2nd tab in the Safari browser.
4	You want to test this MFA method on your smartphone. Open the Safari browser on your smartphone and log in to the university website.
5	You want to test this MFA method on a lab computer. Use the provided lab computer and log in to the university website (2nd tab in the browser).

Appendix B.
Pre-Study Questionnaire

B.1. Previous Experience:

Table 2. QUESTIONS FOR PREVIOUS EXPERIENCE.

No.	Question
1	Have you already had experience with passwordless authentication? (i) Yes, (ii) No
2	Have you already had experience with multi-factor authentication (MFA)? (i) Yes, (ii) No
3	If yes, what types of MFA have you already used? 1) Push notifications on a smartphone 2) Confirmation codes via authentication app (e.g., Google Authenticator, FreeOTP) 3) Biometric methods (e.g., fingerprint) 4) Confirmation codes via SMS 5) Confirmation codes via email 6) Hardware security key (e.g., Yubikey, Solokey)

B.2. Affinity for Technology Interaction (ATI):

In the following, we will ask you about your interaction with technical systems. The term "technical systems" refers to apps and other software applications, as well as entire digital devices (e.g., Mobile phone, computer, TV, car navigation). Please indicate the degree to which you agree/disagree with the following statements. There are no right or wrong answers. (Completely disagree; Largely disagree; Slightly disagree; Slightly agree; Largely agree; Completely agree)

Table 3. QUESTIONS FOR AFFINITY FOR TECHNOLOGY INTERACTION (ATI).

No.	Statement
1	I like to occupy myself in greater detail with technical systems.
2	I like testing the functions of new technical systems.
3	I predominantly deal with technical systems because I have to.
4	When I have a new technical system in front of me, I try it out intensively.
5	I enjoy spending time becoming acquainted with a new technical system.
6	It is enough for me that a technical system works; I don't care how or why.
7	I try to understand how a technical system exactly works.
8	It is enough for me to know the basic functions of a technical system.
9	I try to make full use of the capabilities of a technical system.

B.3. Privacy Concern (PC):

Please state how much you agree or disagree to the following statements. There are no right or wrong answers. (Strongly disagree; Disagree; somewhat disagree; Neither disagree nor agree; somewhat agree; Agree; Strongly agree.)

Table 4. QUESTIONS FOR PRIVACY CONCERN (PC).

No.	Statement
1	I am concerned that companies are collecting too much information about me.
2	I am concerned about my privacy.
3	To me it is important to keep my privacy intact.
4	Novel technologies are threatening privacy increasingly.

B.4. Demographic Questions:

Table 5. DEMOGRAPHIC QUESTIONS.

No.	Question
1	Please indicate your age group. (i) under 20, (ii) 20-29, (iii) 30-39, (iv) 40-49, (v) 50-59, (vi) 60-69, (vii) 70+
2	Which gender do you identify with? (i) Female, (ii) Male, (iii) Other, (iv) No answer
3	What is your highest educational degree? (i) Intermediate school, (ii) High school diploma, (iii) Bachelor's degree, (iv) Master's degree, Diploma, (v) Doctorate
4	Do you have an IT/computer science background? (i) Yes, (ii) No
5	Which persona group do you belong to at the university? (i) Student, (ii) Administrative staff, (iii) Faculty/Academic staff

Appendix C.
Post-Study Questionnaire

Usability: Please state your level of agreement or disagreement for the following statements based on your experience with the presented authentication method. There are no right or wrong answers. (Strongly disagree; Disagree; Neither disagree nor agree; Agree; Strongly agree.)

Table 6. QUESTIONS FOR SYSTEM USABILITY SCALE.

No.	Statement
1	I think that I would like to use this system frequently.
2	I found the system unnecessarily complex.
3	I thought the system was easy to use.
4	I think that I would need the support of a technical person to be able to use this system.
5	I found the various functions in this system were well integrated.
6	I thought there was too much inconsistency in this system.
7	I would imagine that most people would learn to use this system very quickly.
8	I found the system very awkward to use.
9	I felt very confident using the system.
10	I needed to learn a lot of things before I could get going with this system.

Acceptance: Please judge the authentication method on the following adjectives. There are no right or wrong answers.

Table 7. QUESTIONS FOR ACCEPTANCE.

First Adjective	Scale					Second Adjective
	◯	◯	◯	◯	◯	
Useful	◯	◯	◯	◯	◯	Useless
Pleasant	◯	◯	◯	◯	◯	Unpleasant
Bad	◯	◯	◯	◯	◯	Good
Nice	◯	◯	◯	◯	◯	Annoying
Effective	◯	◯	◯	◯	◯	Superfluous
Irritating	◯	◯	◯	◯	◯	Likeable
Assisting	◯	◯	◯	◯	◯	Worthless
Undesirable	◯	◯	◯	◯	◯	Desirable
Raising alertness	◯	◯	◯	◯	◯	Sleep-inducing

Appendix D. Interview Questions

Table 8. INTERVIEW QUESTIONS.

No.	Question
1	How would you describe your user experience with the MFA method you just used?
2	What advantages do you see in using the tested MFA method?
3	What disadvantages do you see in using the tested MFA method?
4	Would you want to use the tested MFA method for your current activities at the university? If yes, why? If no, why not?
5	Would you want to use the tested MFA method privately? If yes, why and for which types of accounts? If no, why not?
6	Do you use MFA methods or password management measures both professionally and privately?
7	Would you replace your current methods with the one tested today, if possible?
8	Suppose you use this method for your university account. How would you assess its security, especially if you lose the smartphone/security key?
9	How do you assess the impact of losing the smartphone/security key on your own access to your university account?
10	The integration of the method varied slightly across devices. What is your opinion on this, or do you even have a preference?

Appendix E. Regression Model SUS

Table 9. REGRESSION MODEL SUMMARY FOR SUS SCORES INCLUDING R, R^2, ADJUSTED R^2, AND F-STATISTIC.

	R	R²	Adjusted R²	F
H_1	0.540	0.292	0.250	$F(5, 86) = 7.082$ $\mathbf{p < .001}$

Table 10. REGRESSION MODEL PREDICTORS FOR SUS SCORES. PREDICTORS ARE DISPLAYED WITH b (UNSTANDARDIZED REGRESSION COEFFICIENT), SE (STANDARD ERROR OF THE COEFFICIENT), AND T-STATISTIC.

Predictor	b	SE	t	p
Intercept	75.305	6.169	12.208	$< .001$
ATI Score	3.887	1.297	2.996	**.004**
MFA Method (2)	-15.878	3.536	-4.491	$\mathbf{< .001}$
MFA Method (3)	-10.939	3.504	-3.122	**.002**
Role (2)	-5.615	3.559	-1.578	.118
Role (3)	-7.409	3.518	-2.106	**.038**

Appendix F. Regression Model Acceptance

Table 11. REGRESSION MODEL SUMMARY FOR ACCEPTANCE SCORES INCLUDING R, R^2, ADJUSTED R^2, AND F-STATISTIC.

	R	R²	Adjusted R²	F
H_1	0.807	0.652	0.599	$F(12, 79) = 12.335$ $\mathbf{p < .001}$

Table 12. REGRESSION MODEL PREDICTORS FOR ACCEPTANCE SCORES. PREDICTORS ARE DISPLAYED WITH b (UNSTANDARDIZED REGRESSION COEFFICIENT), SE (STANDARD ERROR OF THE COEFFICIENT), AND T-STATISTIC.

Predictor	b	SE	t	p
Intercept	2.020	.477	4.233	$< .001$
Role (2)	$-.194$	.218	$-.888$	.377
Role (3)	$-.284$	.195	-1.458	.149
IT (2)	$-.117$	.119	$-.985$	.327
PC Score	.019	.055	.342	.733
ATI Score	$-.019$	.052	$-.366$	.715
SUS Score	.031	.004	8.603	$\mathbf{< .001}$
MFA Method (2)	-.267	.214	-1.250	.215
MFA Method (3)	-.526	.212	-2.485	**.015**
Role (2) * MFA (2)	.175	.290	.603	.548
Role (3) * MFA (2)	.594	.286	2.077	**.041**
Role (2) * MFA (3)	.220	.301	.733	.466
Role (3) * MFA (3)	.319	.292	1.092	.278

Appendix G.
Qualitative Code Book

A. Changes in Cognitive and Physical Efforts

- A.1 Reduction of Cognitive Effort
  - A.1.1 Not Having to Memorize Passwords
  - A.1.2 PIN Instead of Password
- A.2 Additional Physical Effort
  - A.2.1 Extra Hardware
  - A.2.2 Slower Login Times
  - A.2.3 Having to Type more
- A.3 Reduction of Physical Effort
  - A.3.1 Not Having to Type Passwords or Usernames
  - A.3.2 No Extra Hardware Needed
  - A.3.3 Faster Login Times
- A.4 Changing Habits

B. Perception and Mental Models

- B.1 Security Perception
  - B.1.1 Improvement to Security
  - B.1.2 Questionable Security
- B.2 Privacy Concerns
  - B.2.1 (Mis-) Trust in Big Tech
  - B.2.2 Using Biometrics
- B.3 Recovery Concerns
  - B.3.1 Fear of Being Locked out
  - B.3.2 Fallback Mechanisms
  - B.3.3 IT Support Processes
  - B.3.4 Passkey Syncing Aids Recovery
- B.4 Misconceptions
  - B.4.1 Fingerprint gets sent to the service
  - B.4.2 TOTPs are sent to the phone

C. Restrictions in Applicability

- C.1 Compatibility
  - C.1.1 Universally Compatible
  - C.1.2 Personal Device Setup Not Compatible
- C.2 Suitability in University Use Cases
  - C.2.1 Using Personal Devices in for Work
  - C.2.2 Exam Situations
- C.3 Delegation and Account Sharing

D. Authenticator Characteristics and Accessibility

- D.1 Smartphone Usage
  - D.1.1 Form Factor
  - D.1.2 Biometric Sensor
  - D.1.3 QR Code Scanning
- D.2 Issues with Authenticator App
  - D.2.1 Codes Refreshing
  - D.2.2 Code Management (Deletion and Copying)
  - D.2.3 Switching Between Apps
  - D.2.4 App Fatigue
- D.3 Security Key Form Factor
  - D.3.1 Too Small
  - D.3.2 Attaching to Key Ring
  - D.3.3 Key Facing Downwards
- D.4 Prior Device/OS Experience
- D.5 Cost
- D.6 Accessibility Concerns

E. Opinions and Feedback

- E.1 Affective Perception
  - E.1.1 Positive Feedback
  - E.1.2 Negative Feedback
  - E.1.3 Emotional Reactions
- E.2 Suggestions for Improvement
  - E.2.1 Keyboard Suggestion for OTP
  - E.2.2 Fingerprint Sensor Security Key
  - E.2.3 CDA Improvements
  - E.2.4 Conditional Mediation Discoverability Gap
  - E.2.5 Third-Party Support
- E.3 Integration Across Platforms
  - E.3.1 No Preferences
  - E.3.1 OS Differences in Instructions

F. Usability Challenges

- F.1 Technical Issues
  - F.1.1 Double Enrollment
  - F.1.2 Deleting a Credential from RP
  - F.1.3 Removing Key During Enrollment Process
  - F.1.4 NFC Yubico Demo Page
- F.2 Unclear System Instructions
  - F.2.1 Activate
  - F.2.2 Again

Appendix H.
Overview of Affective Perceptions

Table 13. PARTICIPANTS' AFFECTIVE PERCEPTIONS PER MFA METHOD.

Affective Perception	G_{OTP}	G_{Seckey}	$G_{Passkey}$
Largely Positive	15	14	25
Largely Negative	5	1	0
Mixed	11	15	6
No Clear Perception	5	1	0

Appendix I.
Willingness to Adopt

Table 14. PARTICIPANTS' WILLINGNESS TO ADOPT AN MFA METHOD FOR THEIR UNIVERSITY ACCOUNT, CATEGORIZED INTO FOUR GROUPS: "YES", "MAYBE/DEPENDS", "ALTERNATIVE", AND "NO"

University Account	G_{OTP}	G_{Seckey}	$G_{Passkey}$
Yes	12	19	28
Maybe/Depends	8	2	1
Alternative	7	3	0
No	4	6	2

Table 15. PARTICIPANTS' WILLINGNESS TO ADOPT AN MFA METHOD FOR PERSONAL ACCOUNTS, CATEGORIZED INTO FOUR GROUPS: "YES", "MAYBE/DEPENDS", "ALTERNATIVE", AND "NO"

Personal Accounts	G_{OTP}	G_{Seckey}	$G_{Passkey}$
Yes	14	9	21
Maybe/Depends	6	1	8
Alternative	4	15	1
No	7	12	1

Appendix J.
Visuals of Key Interfaces

J.1. MacOS Security Key Instructions

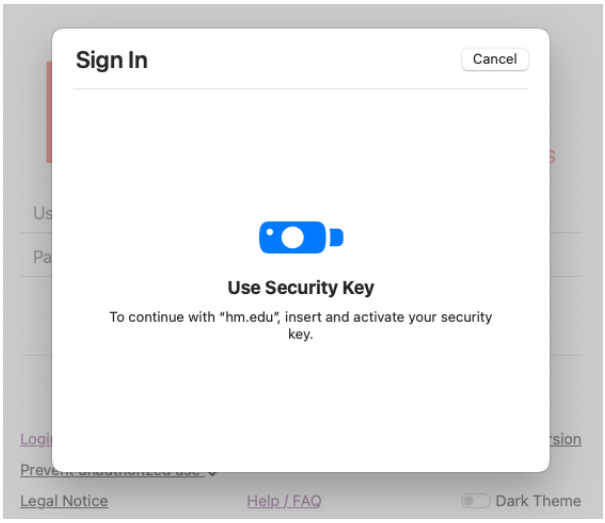

Figure 1. MacOS Security Key Dialog: "activate".

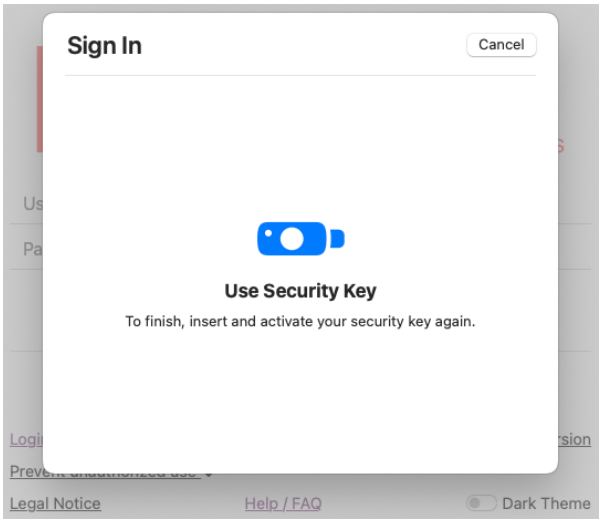

Figure 2. MacOS Security Key Dialog: "insert [...] again".

J.2. Conditional Mediation Discoverability Gap

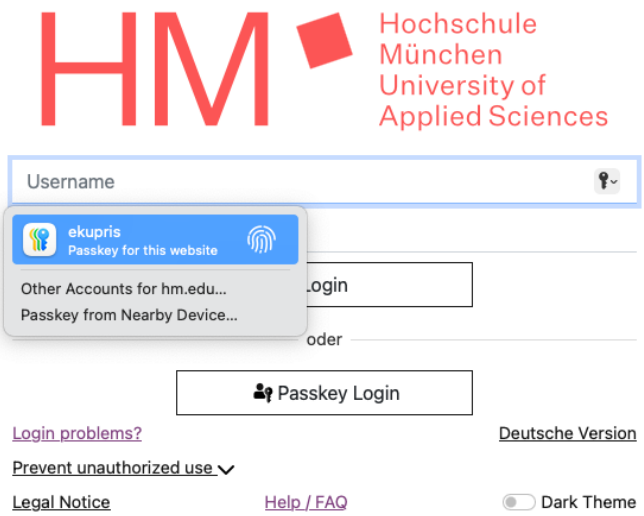

Figure 3. macOS Conditional Mediation Dialog: Participants often overlooked it, especially because it disappears once the user types in anything.

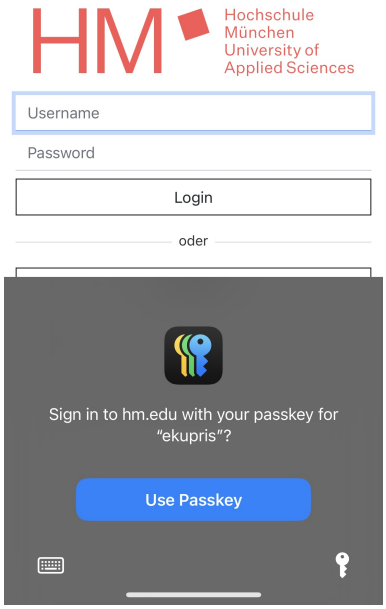

Figure 4. iOS Conditional Mediation Dialog: The autofill prompt takes up a large portion of the phone screen, making it more noticeable.