

“It’s Just a Lot of Prerequisites”

A User Perception and Usability Analysis of the German ID Card as a FIDO2 Authenticator

Markus Keil ¹

Philipp Markert ¹

Markus Dürmuth ²

¹Ruhr University Bochum



²Leibniz University Hannover



September 29-30 | The 2022 European Symposium on Usable Security 2022 | Karlsruhe, Germany

Introduction

eID



Introduction

eID

- electronic **i**dentification system built into German ID cards (“neuer Personalausweis”, nPA)



Introduction

eID

- electronic identification system built into German ID cards (“neuer Personalausweis”, nPA)



Introduction

eID

- electronic identification system built into German ID cards (“neuer Personalausweis”, nPA)



- Full Name
- Date of Birth
- Place of Birth
- Address
- ...

Introduction

eID

- electronic identification system built into German ID cards (“neuer Personalausweis”, nPA)



- Full Name
- Date of Birth
- Place of Birth
- Address
- ...
- *Cryptographic Keys*



Introduction

eID User Environment



Introduction

eID User Environment



Introduction

eID User Environment



Introduction

eID User Environment



Introduction

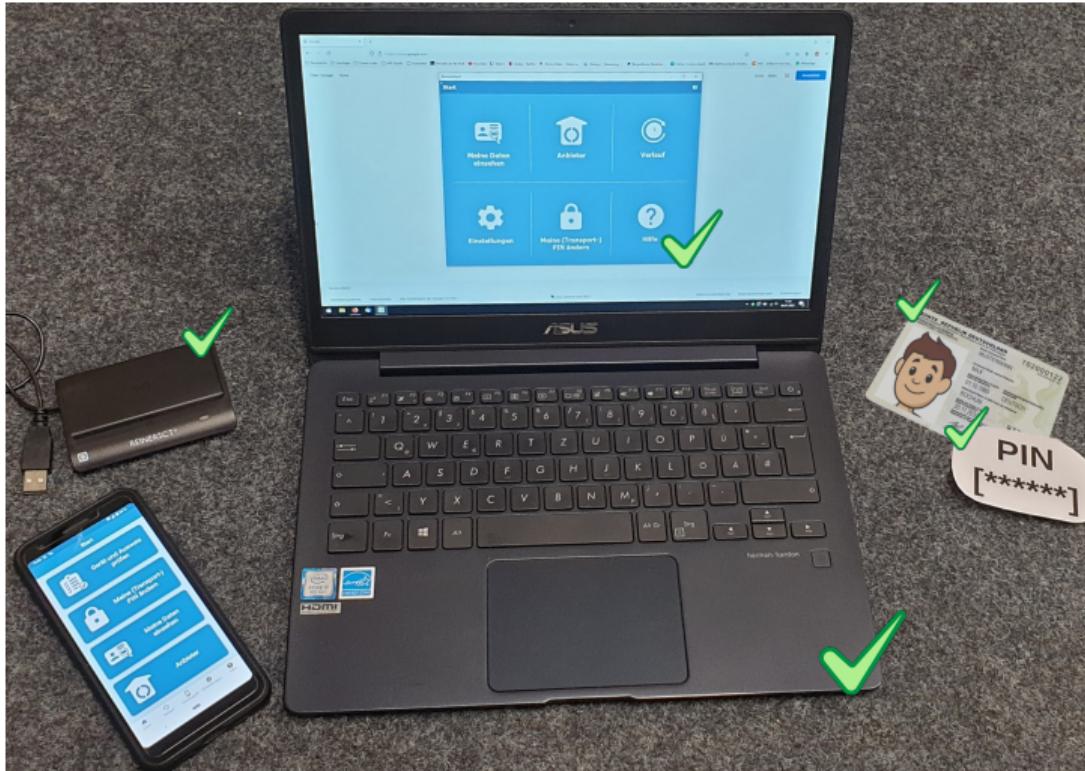
eID User Environment



Introduction

eID User Environment

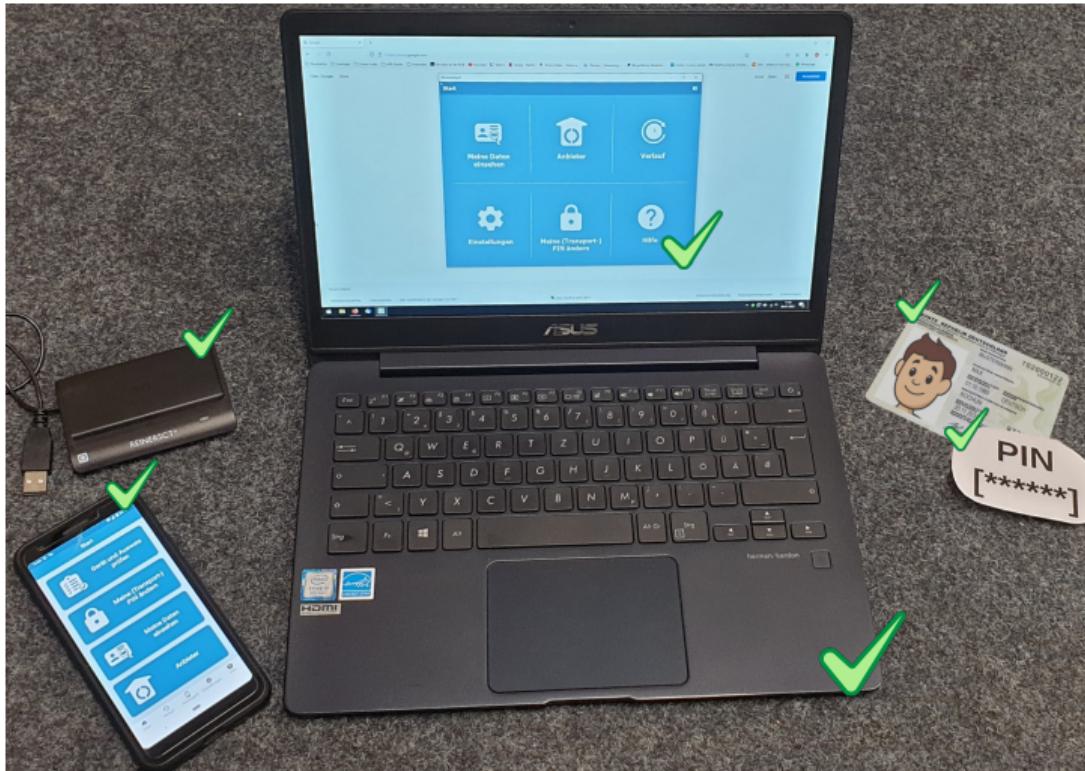
Option 1 ⇒



Introduction

eID User Environment

Option 1 ⇒



Option 2 ⇒

Introduction

FIDELIO

Introduction

FIDELIO



Introduction

FIDELIO



FIDELIO
User Environment =

Introduction

FIDELIO



FIDELIO
User Environment

=



eID User
Environment

+

Introduction

FIDELIO



Research Questions

Research Questions

RQ1 Are users aware of the possibility of using their German ID card as a FIDO2 authenticator?

Research Questions

RQ1 Are users aware of the possibility of using their German ID card as a FIDO2 authenticator?

RQ2 How do users perceive the German ID as a second factor in terms of usability?

Research Questions

- RQ1 Are users aware of the possibility of using their German ID card as a FIDO2 authenticator?
- RQ2 How do users perceive the German ID as a second factor in terms of usability?
- RQ3 Are users accepting the German ID as a second factor?

Research Questions

- RQ1 Are users aware of the possibility of using their German ID card as a FIDO2 authenticator?
- RQ2 How do users perceive the German ID as a second factor in terms of usability?
- RQ3 Are users accepting the German ID as a second factor?
- RQ4 What thoughts and concerns arise in the users' minds when using the German ID as a second factor?

Research Questions

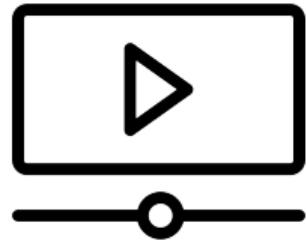
- RQ1 Are users aware of the possibility of using their German ID card as a FIDO2 authenticator?
- RQ2 How do users perceive the German ID as a second factor in terms of usability?
- RQ3 Are users accepting the German ID as a second factor?
- RQ4 What thoughts and concerns arise in the users' minds when using the German ID as a second factor?

Method

Study Structure

Method

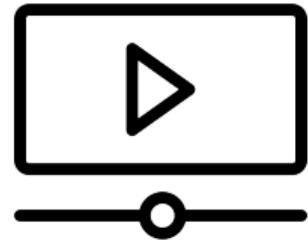
Study Structure



1. Videos

Method

Study Structure



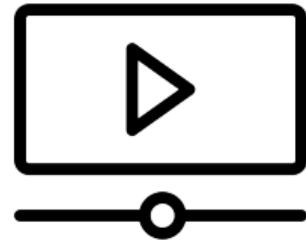
1. Videos



2. Hands-On Tasks

Method

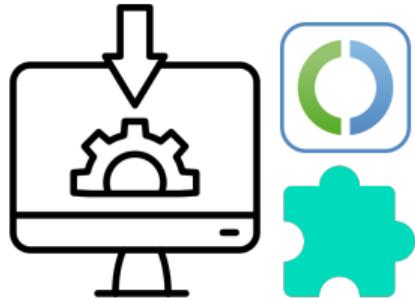
Study Structure



1. Videos

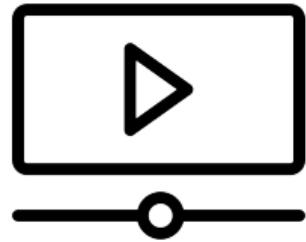


2. Hands-On Tasks



Method

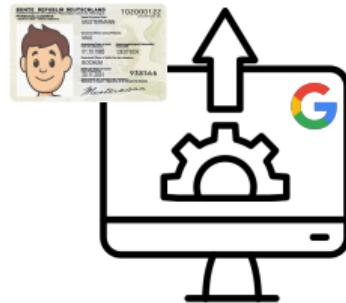
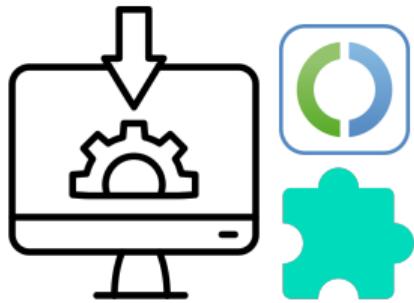
Study Structure



1. Videos

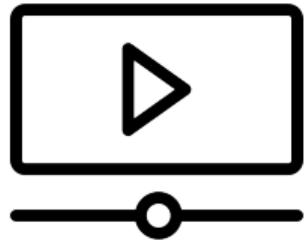


2. Hands-On Tasks



Method

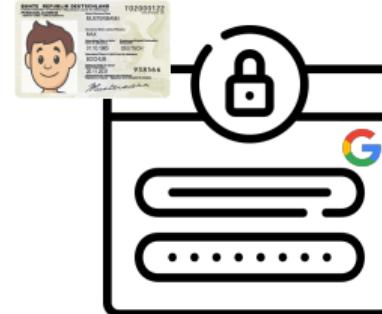
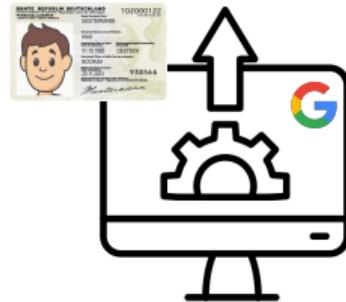
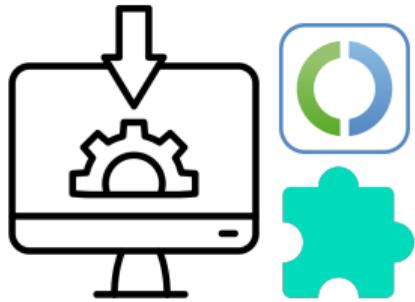
Study Structure



1. Videos

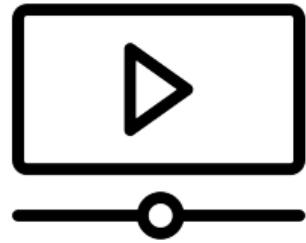


2. Hands-On Tasks



Method

Study Structure



1. Videos



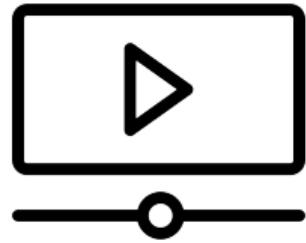
2. Hands-On Tasks



3. Survey

Method

Study Structure



1. Videos



2. Hands-On Tasks



3. Survey



4. Interview

Method

Participant Landscape

	Cardreader	Smartphone

Method

Participant Landscape

	Cardreader	Smartphone
Random	<i>GroupCR1</i>	<i>GroupSM1</i>

Method

Participant Landscape

	Cardreader	Smartphone
Random	<i>GroupCR1</i>	<i>GroupSM1</i>
Tech-Savvy	<i>GroupCR2</i>	<i>GroupSM2</i>

Round 1



10x Random



Round 2



10x Tech-Savvy

Results

RQ2: Perceived Usability

<i>GroupCR1</i>	<i>GroupSM1</i>	<i>GroupCR2</i>	<i>GroupSM2</i>
72	62	75	59



Results

RQ2: Perceived Usability

<i>GroupCR1</i>	<i>GroupSM1</i>	<i>GroupCR2</i>	<i>GroupSM2</i>
72	62	75	59



CR2₁: "I would have had difficulties without the videos."

Results

RQ2: Perceived Usability

<i>GroupCR1</i>	<i>GroupSM1</i>	<i>GroupCR2</i>	<i>GroupSM2</i>
72	62	75	59



CR2₁: "I would have had difficulties without the videos."

SM2₄: "There are too many things that I have to have and use."

Results

RQ2: Perceived Usability

<i>GroupCR1</i>	<i>GroupSM1</i>	<i>GroupCR2</i>	<i>GroupSM2</i>
72	62	75	59



CR2₁: “I would have had difficulties without the videos.”

SM2₄: “There are too many things that I have to have and use.”

Results

RQ4: Thoughts and Concerns

Results

RQ4: Thoughts and Concerns

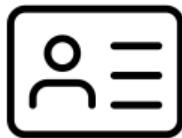
SM2₃: “Virtually everyone owns a smartphone and basically every German citizen has an ID card, meaning that the system is always available as a second factor.”



Results

RQ4: Thoughts and Concerns

SM2₃: “Virtually everyone owns a smartphone and basically every German citizen has an ID card, meaning that the system is always available as a second factor.”



CR1₃: “It's just a lot of prerequisites, always having my ID card with me and remembering my PIN”

Results

RQ4: Thoughts and Concerns

SM2₃: “Virtually everyone owns a smartphone and basically every German citizen has an ID card, meaning that the system is always available as a second factor.”



CR1₃: “*It's just a lot of prerequisites*, always having my ID card with me and remembering my PIN”

SM1₂: “Yes, I could imagine [using it for] finance accounts, there is no way I would use it for social media [...]”



Results

RQ4: Thoughts and Concerns

Results

RQ4: Thoughts and Concerns

CR1₅: “I don't know what happens with the data that is read from the chip, especially when Google does it.”



Results

RQ4: Thoughts and Concerns

CR1₅: “I don't know what happens with the data that is read from the chip, especially when Google does it.”



“What data do you think is shared with the services that you register with?”

Results

RQ4: Thoughts and Concerns

CR1₅: “I don't know what happens with the data that is read from the chip, especially when Google does it.”



Round 1

“What data do you think is shared with the services that you register with?”

Results

RQ4: Thoughts and Concerns

CR1₅: “I don't know what happens with the data that is read from the chip, especially when Google does it.”



Name
Date of Birth
Nationality
Address

Date of Expiry
Date of Issue
None

Round 1

“What data do you think is shared with the services that you register with?”

Round 2

Results

RQ4: Thoughts and Concerns

CR1₅: "I don't know what happens with the data that is read from the chip, especially when Google does it."



Name
Date of Birth
Nationality
Address

Date of Expiry
Date of Issue
None

Round 1

"What data do you think is shared with the services that you register with?"

Round 2

SM2₁: "I only checked the box for the date of expiry because I thought the second factor could expire [...]."

Discussion

Discussion



Security Misconceptions

Discussion



Security Misconceptions

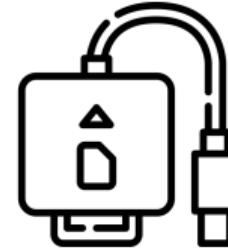


Smartphone vs Cardreader

Discussion



Security Misconceptions



Smartphone vs Cardreader

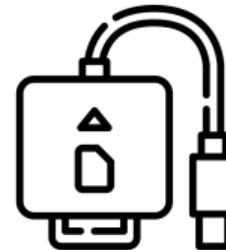


Currently No Ongoing Support

Discussion



Security Misconceptions



Smartphone vs Cardreader



Currently No Ongoing Support



Promising Concept

Summary

Summary

FIDELIO

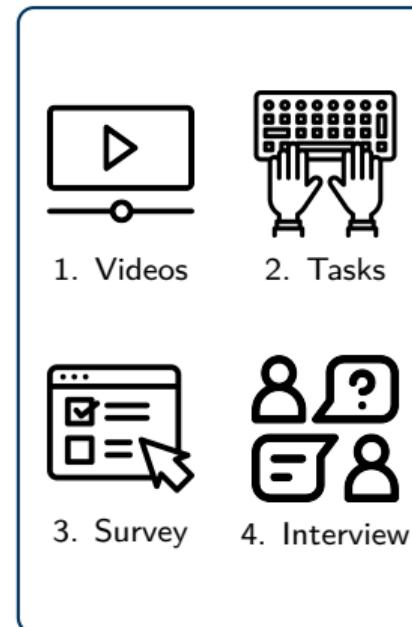


Summary

FIDELIO



Study Design

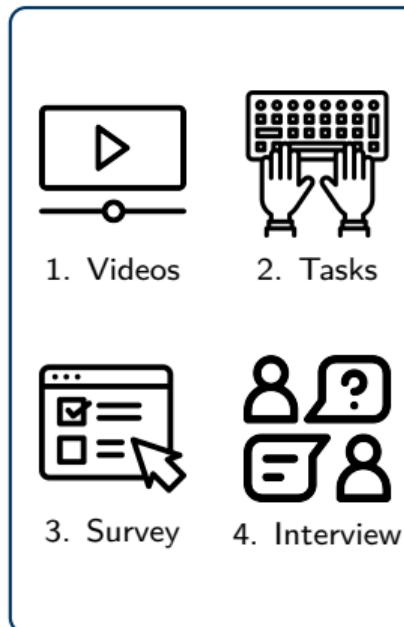


Summary

FIDELIO



Study Design



Conclusion

- 👎 Difficulties in Setup
- 👎 Unnecessarily Complex Steps
- 👎 Security Misconceptions
- 👍 Promising Concept

markus.keil@rub.de

Awareness

	Round 1	Round 2
Did you know about eID?	8	9
Did you know about FIDO2?	1	1
Have you used eID before?	1	2

Survey Scores

	Round 1		Round 2	
	<i>Group_{CR1}</i>	<i>Group_{SM1}</i>	<i>Group_{CR2}</i>	<i>Group_{SM2}</i>
SUS	72	62	75	59
Acceptance				
Usefulness	1.2	1.0	1.1	0.7
Satisfying	0.8	0.5	1.1	0.2
ATI	3.5	3.3	4.2	4.8
Privacy Concerns	4.6	5.3	5.4	5.2

Run Timings

	Round 1		Round 2	
	<i>Group_{CR1}</i>	<i>Group_{SM1}</i>	<i>Group_{CR2}</i>	<i>Group_{SM2}</i>
Min	3:28	5:57	4:25	5:14
Max	11:08	21:50	8:12	11:22
Range	7:40	15:53	3:47	6:08
Mean	7:47	16:15	5:49	7:21
Median	8:00	18:08	5:20	5:55
Standard Deviation	2:30	5:43	1:23	2:16

Demographics

		Round 1		Round 2	
		<i>Group_{CR1}</i>	<i>Group_{SM1}</i>	<i>Group_{CR2}</i>	<i>Group_{SM2}</i>
Gender	Woman	3	5	4	1
	Man	2	0	1	4
Degree	High School	3	5	3	2
	Bachelor's	2	0	0	1
	Master's	0	0	1	2
	Doctoral	0	0	1	0
Age	18–24	3	4	3	3
	25–34	1	0	2	2
	35–44	1	1	0	0
Tech	Yes	1	1	5	5
	No	4	4	0	0

Individual Scores Round 1

	<i>CR1₁</i>	<i>CR1₂</i>	<i>CR1₃</i>	<i>CR1₄</i>	<i>CR1₅</i>	<i>SM1₁</i>	<i>SM1₂</i>	<i>SM1₃</i>	<i>SM1₄</i>	<i>SM1₅</i>
SUS	50	83	70	93	63	18	73	70	63	85
Acceptance										
Usefulness	1.0	1.6	0.8	2.0	0.8	-0.2	1.6	1.0	1.2	1.4
Satisfying	0.5	1.3	0.3	2.0	0.0	-1.0	1.0	0.8	1.0	0.8
ATI	4.2	4.8	2.4	5.0	1.0	2.8	2.9	4.0	1.8	4.9
PC	5.3	3.5	4.3	4.8	5	5.5	5.8	6.0	3.8	5.3
Partial Task Timings										
Install AusweisApp2	1:15	0:39	0:36	0:50	0:58	1:12	0:43	0:48	1:09	0:53
Install Plugin	0:35	0:30	0:24	2:20	0:59	1:07	0:30	1:08	4:37	0:38
Connect Smartphone	na	na	na	na	na	3:57	3:11	1:00	1:40	0:28
Navigate Google	1:30	2:22	1:06	2:00	2:17	7:57	4:45	1:16	5:43	1:09
Total Completion Time	11:08	7:23	3:28	8:00	8:55	21:50	18:08	14:35	20:44	5:57

Individual Scores Round 2

	<i>CR2₁</i>	<i>CR2₂</i>	<i>CR2₃</i>	<i>CR2₄</i>	<i>CR2₅</i>	<i>SM2₁</i>	<i>SM2₂</i>	<i>SM2₃</i>	<i>SM2₄</i>	<i>SM2₅</i>
SUS Acceptance	35	80	93	88	80	40	70	60	53	73
Usefulness	0.2	0.8	2.0	1.6	1.0	0.4	0.8	0.0	0.8	1.6
Satisfying	0.3	0.5	2.0	2.0	1.0	-0.5	0.3	0.3	-0.3	1.5
ATI	4.6	5.6	4.2	2.0	4.4	5.4	4.6	5.2	5.0	3.9
PC	5.6	5.0	4.0	5.5	6.5	6.3	5.3	4.0	4.8	5.5
Partial Task Timings										
Install AusweisApp2	1:04	0:45	0:56	1:25	0:45	0:42	0:44	0:55	0:51	0:45
Install Plugin	0:25	0:39	0:33	0:52	1:15	0:15	0:26	0:21	0:25	1:01
Connect Smartphone	na	na	na	na	na	1:23	1:20	1:10	1:02	1:16
Navigate Google	1:42	1:28	1:23	2:00	1:50	0:50	1:14	1:09	1:00	1:25
Total Completion Time	4:41	5:20	4:25	6:26	8:12	5:14	8:22	5:55	5:54	11:22

Security Misconceptions

Table: "What data do you think is shared with the services you register with?"

	Round 1			Round 2		
	<i>Group_{CR1}</i>	<i>Group_{SM1}</i>	Combined	<i>Group_{CR2}</i>	<i>Group_{SM2}</i>	Combined
Name	4	5	9	1	2	3
Date of Expiry	3	5	8	3	3	6
Date of Birth	4	3	7	1	1	2
Nationality	2	4	6	1	0	1
Address	4	2	6	1	0	1
Date of Issue	2	4	6	0	3	3
Place of Birth	2	3	5	1	0	1
Height	0	3	3	1	0	1
Colour of Eye	0	2	2	0	0	0
None of the Above	1	0	1	2	1	3