

Guidance in the evaluation of authentication systems

-> Study on the usefulness and impact



Expert Survey

Authentication Mechanisms

mobile connect: user authentication and identity service based on the OpenID Connect/OAuth2 standards (matching the end user to their mobile phone number)

password: process that involves a user entering a unique ID and key that are then checked against stored credentials

sms OTP: a numeric or alphanumeric code is sent to a mobile number

app OTP: a numeric or alphanumeric code is generated by a mobile application

Solution A

- First authentication attempt with mobile connect if activated, otherwise with password

 **session opened**

- Confirmation (**re-authentication**) with mobile connect if activated, otherwise with password
 - after too prolonged **inactivity** (user's choice: 15 minutes/ 2 months)
 - if **session expires** (user's choice: 24 hours/ 6 months)

Solution B

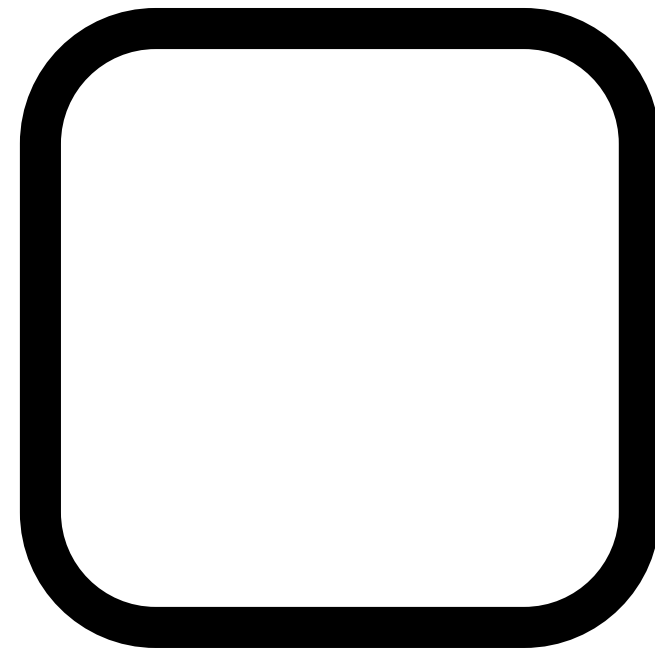
- First authentication attempt with mobile connect if activated, otherwise with password

 **session opened**

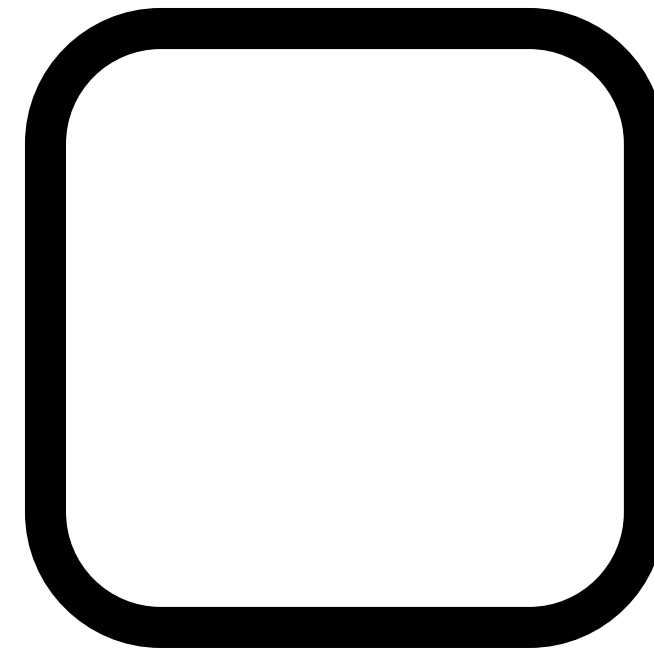
- For every following authentication attempt, a **confidence level** is calculated: if the confidence is not sufficient for the requested resource, a **confirmation (re-authentication)** is requested
 - With mobile connect if activated
 - With application (OS) + password if the application is installed
 - With SMS OTP if a mobile subscription is available
 - With a connection behind the Livebox if Livebox is available
 - DENY

Q1

In your opinion, which of the two solutions seems to be the better one?

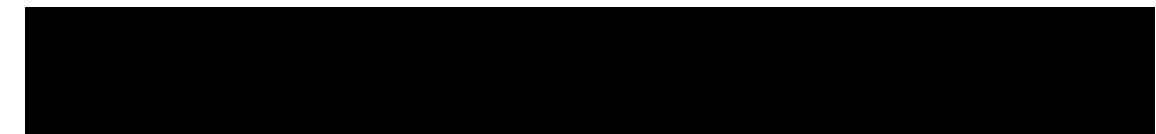
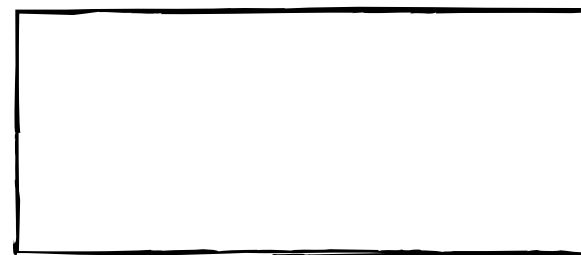


Solution A



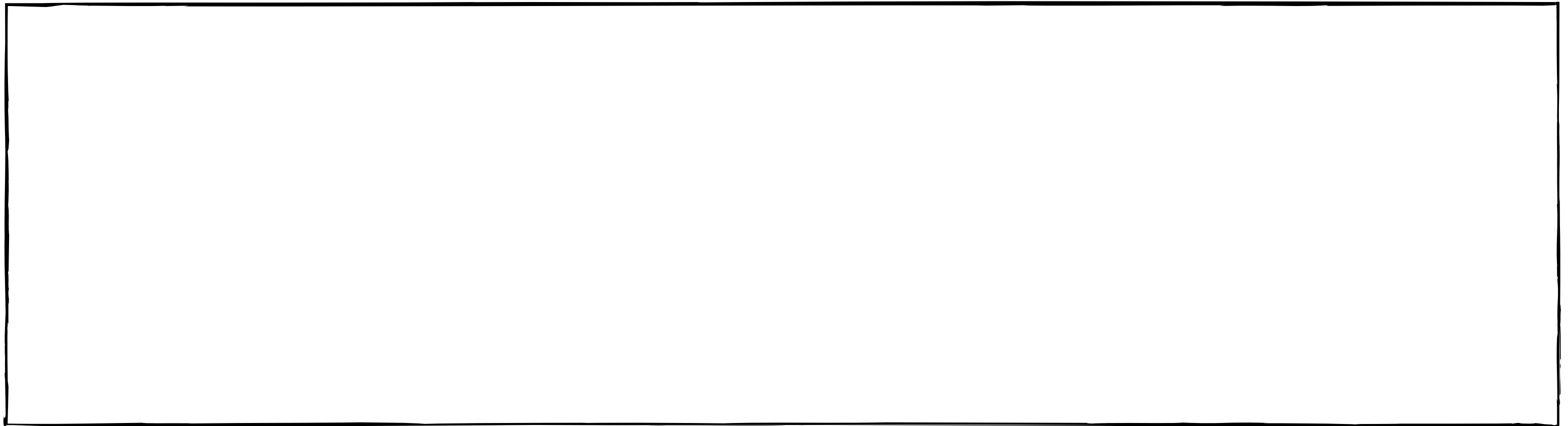
Solution B

time:

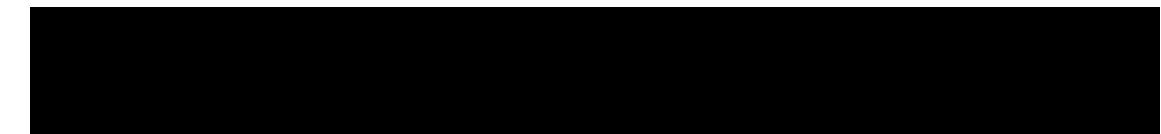
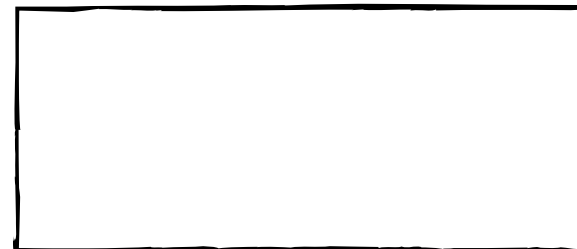


Q2

Which are the reasons why you prefer this solution? According to which criteria did you compare the solutions?

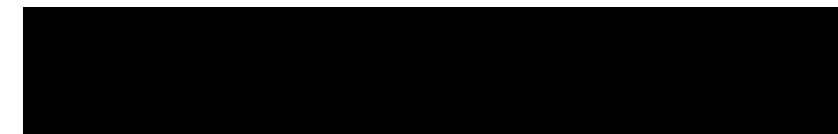


time:



Q3

To what extent (1-5) was it difficult to compare the solutions?
Why?

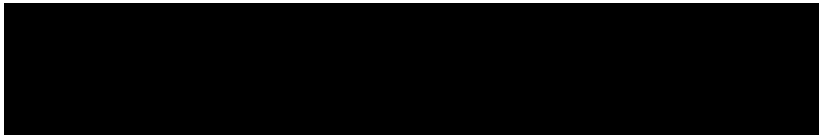


Q4

For the following criteria, which solution seems to be the better one?

	Solution A	Solution B	?
security			
usability			
privacy			
deployability			

time:



Q5

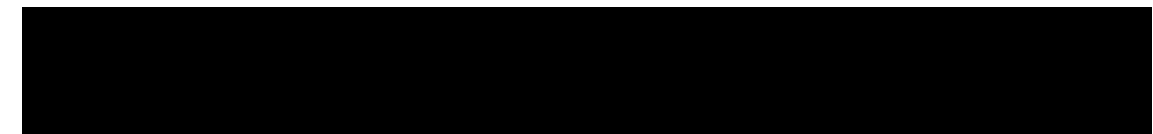
To what extent (1-5) do you agree that the following criteria are crucial for evaluating the solutions?

security

usability

privacy

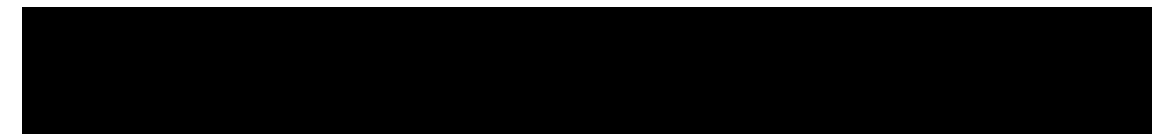
deployability



Q6

Which other criteria do you consider important for evaluating the systems?

time:



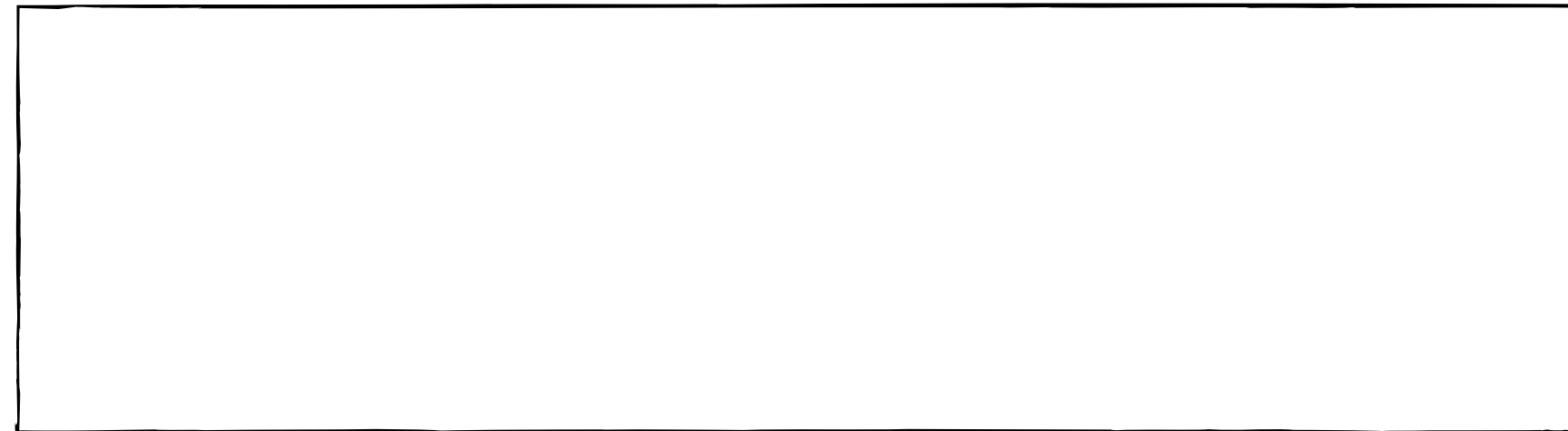
Authentication Path



Q7

For the example user path, are you able to describe the security and the usability ?

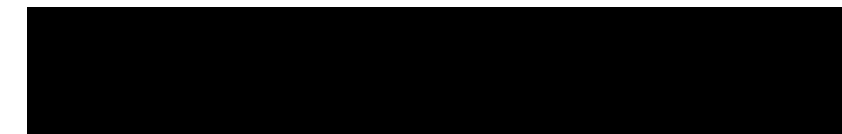
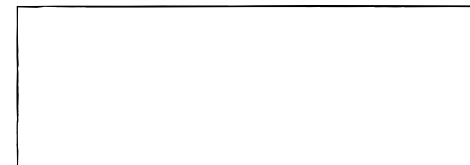
security



usability

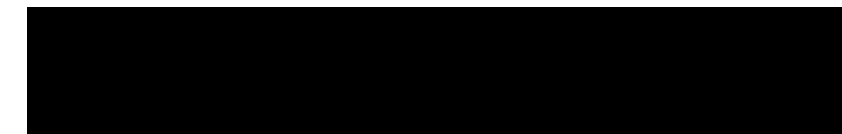
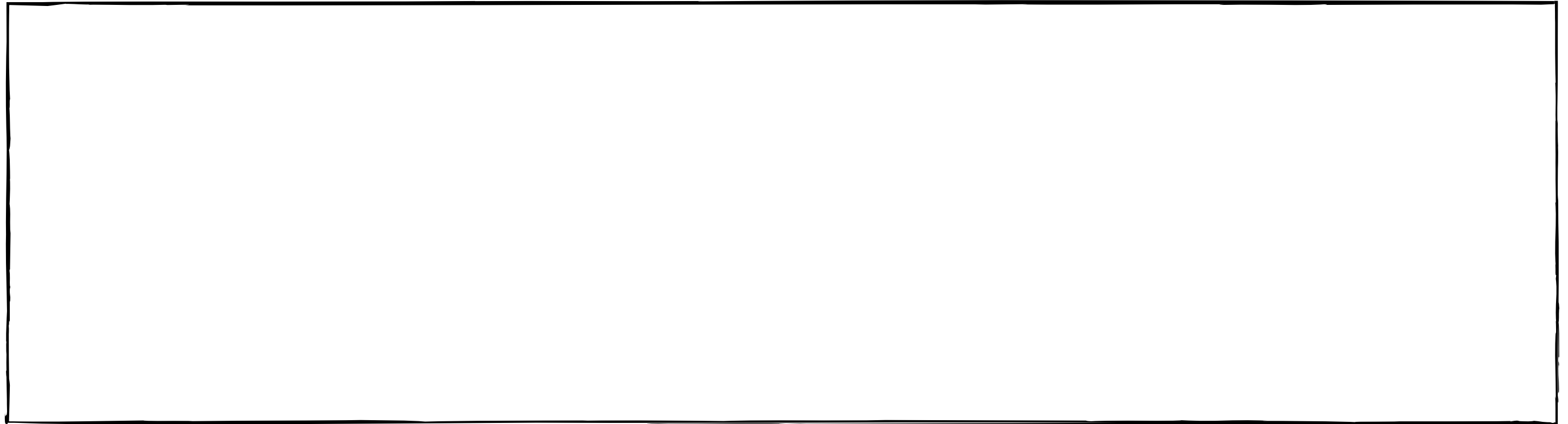


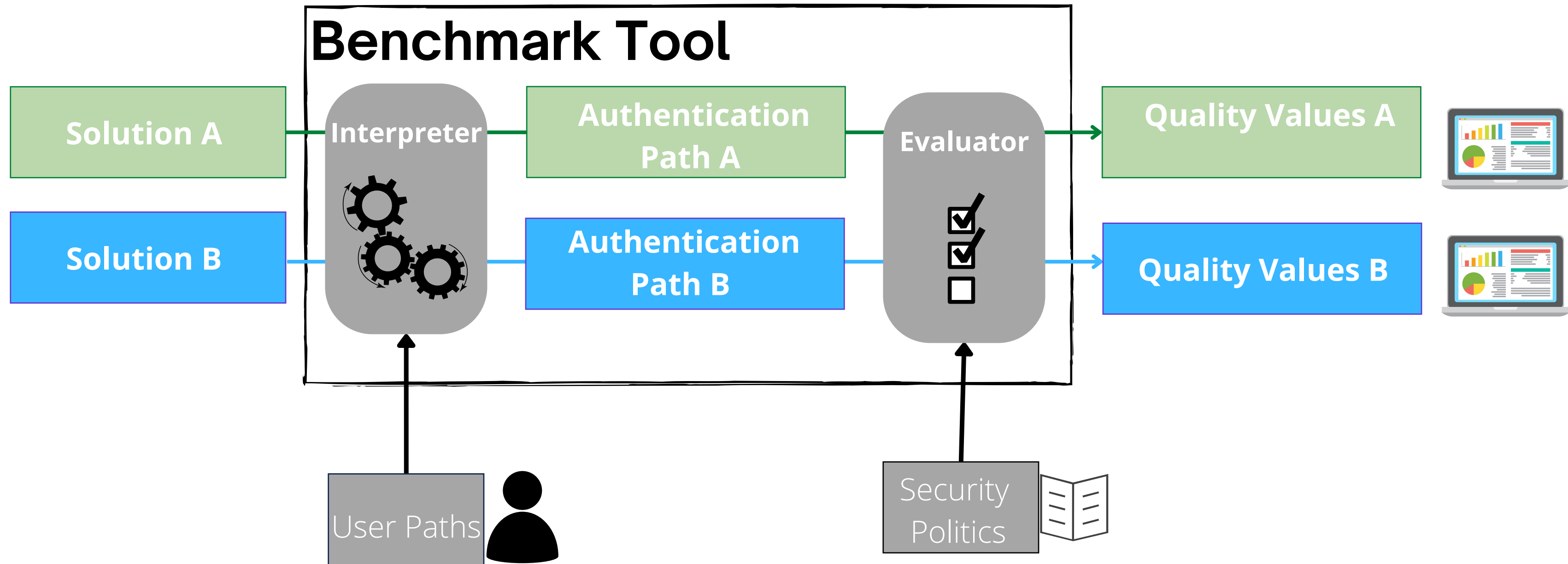
time:



Q8

To what extent (1-5) was it difficult to to describe the security and the usability of the example user path? Why?





*login feature data of more
than 33 million login
attempts and more than
3.3 million users,
login attempts Orange*

*taxonomy to date on the desirable
properties of authentication methods
concerning security, privacy, deployability
and usability*

Solution A

user authentication attempts: 571

number of authentications: 40

usability: [3,3] -> mean=3

("noAdditionalNetworkAccess", "nothingToCarry", "affinityToUser")

security: [1,1] -> mean=1

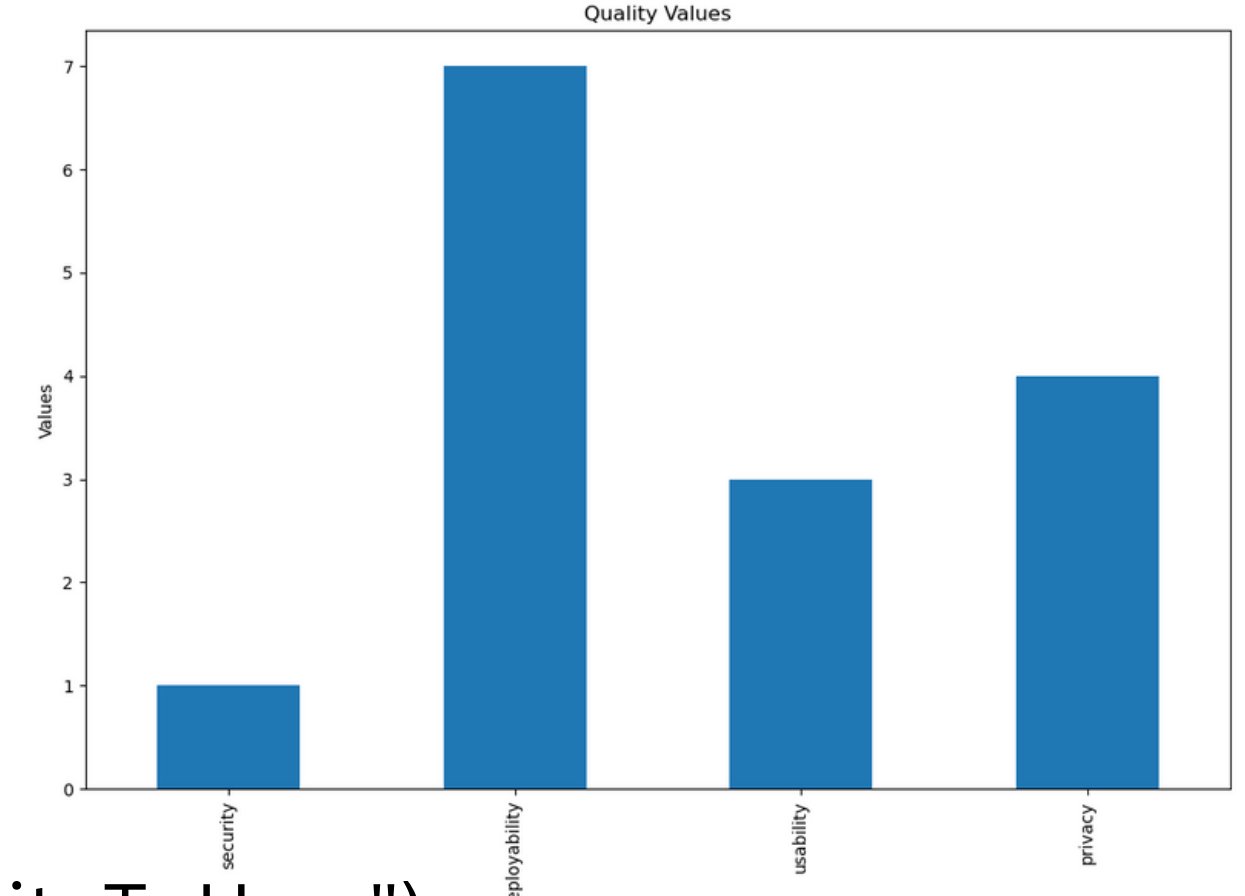
("resilientToPhysicalTheft")

deployability: [7,7] -> mean=7

("browserCompatible", "negligibleImplementationCosts" "negligibleCostsPerUser",
"serverCompatible", "accessible", "mature")

privacy: [4,4] -> mean= 4

("informationCollection", "userAnonymity", "userPersonalDetails", "informationSensitivity")



Solution B

user authentication attempts: 571

number of authentications: 34

usability: [2,7.5] -> mean=5.9

("noAdditionalNetworkAccess", "nothingToCarry", "affinityToUser", "memorywiseEffortless", "infrequentErrors", "notTooComplex")

security: [0,4] -> mean=1.125

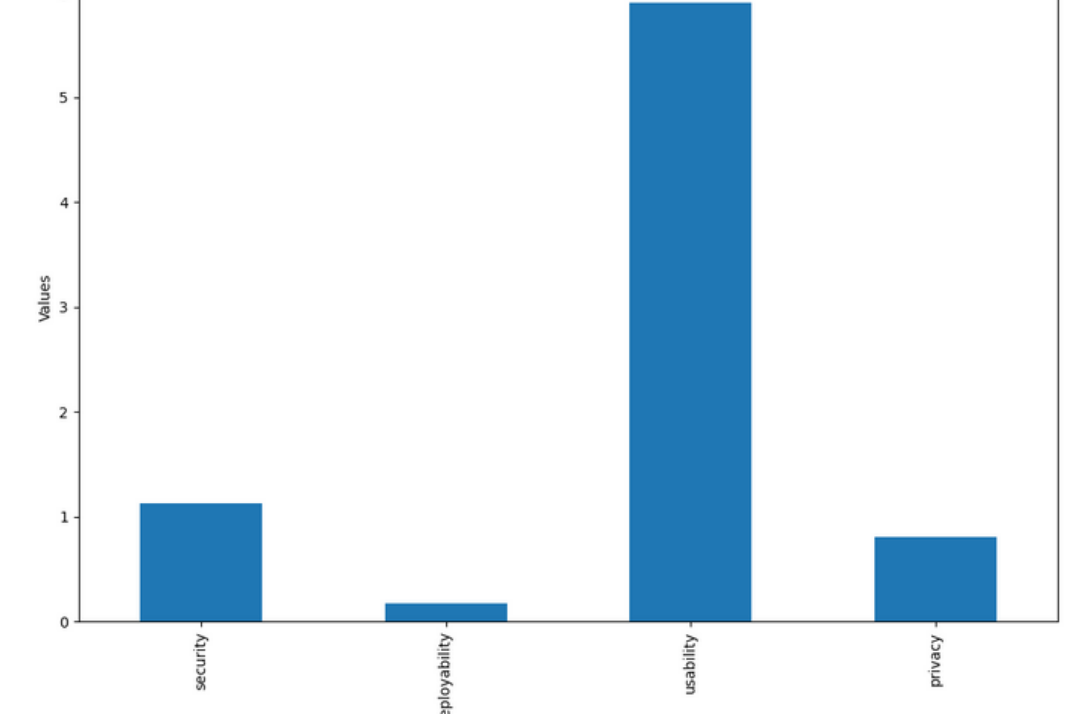
("resilientToPhysicalTheft", "resilientToPhising", "resilientToThrottledGuessing", "resilientToLeaksFromOtherVerifiers", "resilientToObservation")

deployability: [0,7] -> mean=0.175

("browserCompatible", "negligibleImplementationCosts" "negligibleCostsPerUser", "serverCompatible", "accessible", "mature", "nonPropriarity")

privacy: [0,4] -> mean= 0.8

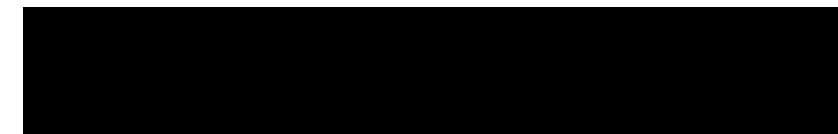
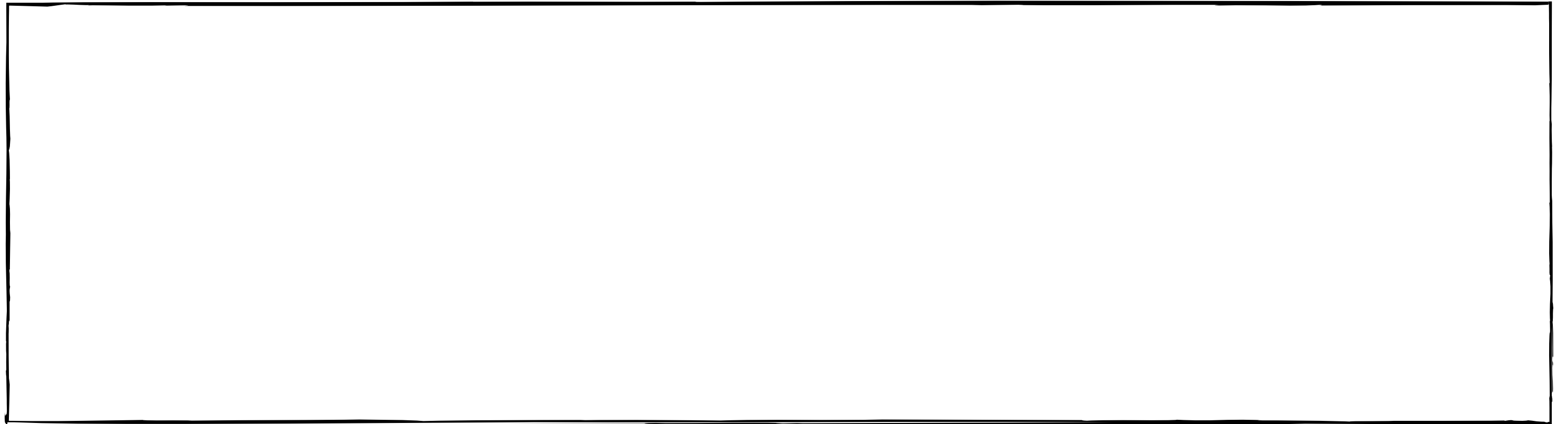
("informationCollection", "userAnonymity", "userPersonalDetails", "informationSensitivity")



	Solution A	Solution B
security	3	5.9
usability	1	1.125
privacy	4	0.8
deployability	7	0.175

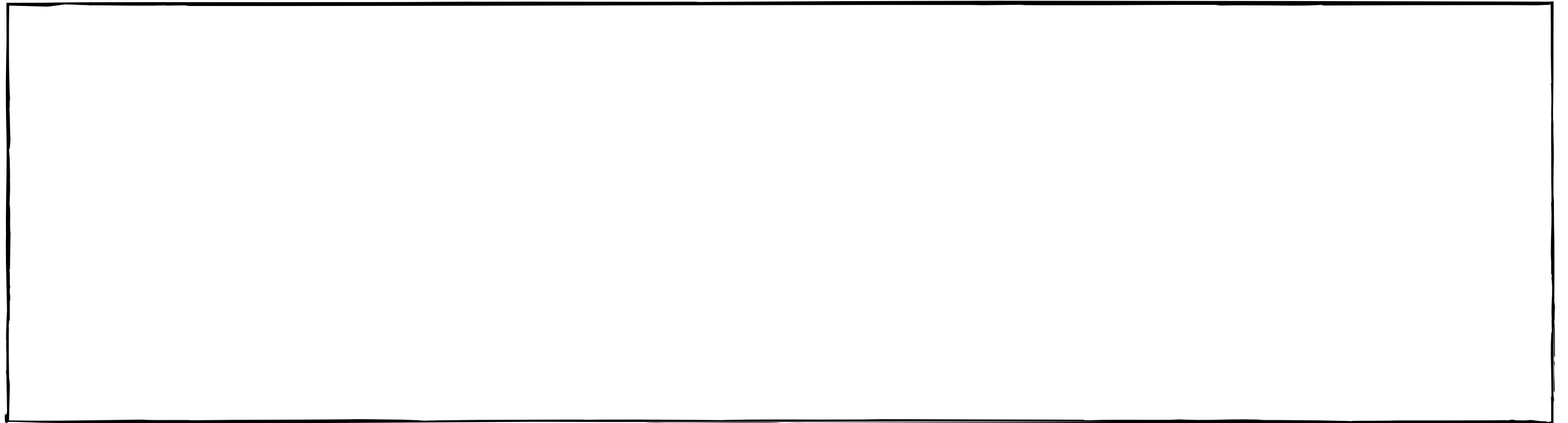
Q9

Do you think the benchmark tool is useful? Why?



Q10

Do you think the extensibility of the benchmark tool is useful?
Why?

A large, empty rectangular box with a thin black border, intended for the user to provide their answer to the question.

Q11

Do you think the benchmark would influence your decisions when it comes to decide about the integration of new authentication solutions? How?

