LUT University
School of Engineering Science
Software Engineering Degree Program

Password-Free Login, mobile application

Group 23, Lappeenranta

Aapo Hyyryläinen aapo.hyyrylainen@student.lut.fi
Arttu Korpela arttu.korpela@student.lut.fi
Joona Kuutniemi joona.kuutniemi@student.lut.fi
Tommi Nykänen tommi.nykanen@student.lut.fi

TABLE OF CONTENTS

IMAGES

METADATA

	PLAN	UNDERSTAND	DESIGN	PRODUCE	EVALUATE
ARTTU	2,5	5	8	9	4
TOMMI	2,5	4,0	4	6	6
JOONA	4,5	3	6	3	5
AAPO	5	4	8	2	6

PLAN
AAPO – Problem description, project motivation, group organisation
TOMMI – User Survey
JOONA – Benchmark research
ARTTU – Group discussion

UNDERSTAND

AAPO – Empathy mapping, user journey
TOMMI – Personas, Affinity mapping
JOONA – Affinity mapping, personas
ARTTU –Empathy mapping, context, user research findings

DESIGN

AAPO – Brainstorming, group discussion
TOMMI – Feedback, group discussion
ARTTU- Paper- and Figma prototypes

PRODUCE

AAPO – Colour coding, tweaks and ideas
TOMMI – design ideas
JOONA – Ideate
ARTTU – Coding

EVALUATE

AAPO – Questionnaire and result analysis
TOMMI – Heuristic evaluations
JOONA – heuristic evaluation findings
ARTTU– Implementing findings to flutter

1. PLANNING

1.1 Problem Definition

A password or a login code can be used to authenticate for a specified system using a known set of keys to enter a phrase or series of numbers. Usually, services also require the password to be complex enough to pass a rudimentary test and as such, make remembering the phrase or series harder for the user. To add to this, a user typically will create multiple accounts for many different services and cannot be bothered to use different passwords that are each harder to remember than the last. This results in either forgetting passwords for certain accounts or using simple passwords that can be easily stolen and used by potential attackers. Passwords are also becoming more obsolete due to technical advances in cracking methods and devices. (Bo, Xinxin, Guang 2014.)

As applications and their technologies become more mature, people are also finding passwords riddled with security issues and annoyance to the user (Bonneau, Herley, van Oorschot, Stajano 2012). The issue can then be divided into two different main categories: Authenticating and making the authentication experience better for the user. As Bonneau et al (2012) present the issue, a lot of the research is based on making analysis and schemes for authentication but fail to account for the realistic use of the authentication software. Both Bo et al (2014) and Bonneau et al (2012) present password-free login as a more suitable, modern option for authentication as it is effortless, scalable and less liable to common security risks.

1.2 Project Goal

In the modern age of applications, social media and even bank access being tied to login codes and passwords, there is rising interest in alternative options for authenticating services. A password-free login hopes to solve the problem with traditional passcodes using ease of access, fast authentication and safety knowing that the authentication cannot be copied or transferred.

The scope of this project is the user interface and user experience of password-free login applications and will discuss different methods of authentication in terms of understanding

the UX of the solution proposed. The project will not attempt to solve authentication or security issues in the methods proposed, but instead deliver a concise solution for developing a password-free login user interface. The result is a concise report on the problems found and digital prototyping of the final ideation during the project. Our group decided upon this project topic as we thought there is room for improvement in the user experience of authentication systems and especially the ease of use of them.

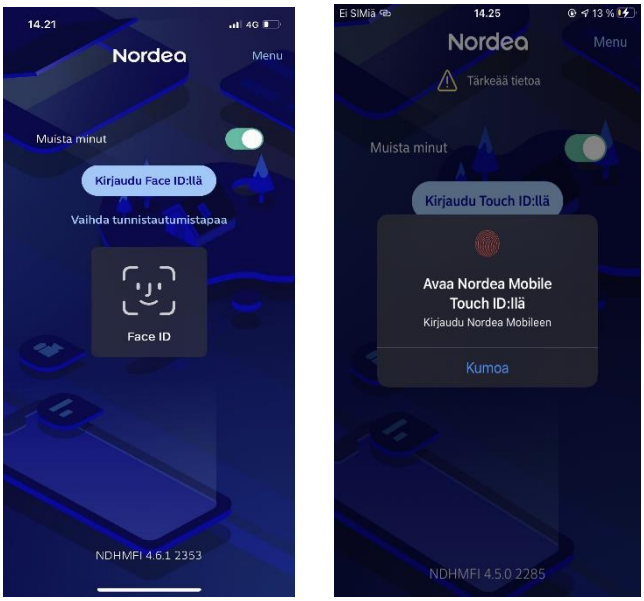
BENCHMARK RESEARCH

- **Apple pay [Face ID]**

1. Benchmark, Apple pay

  - Simple and clear design without anything extra
  - Fast usage

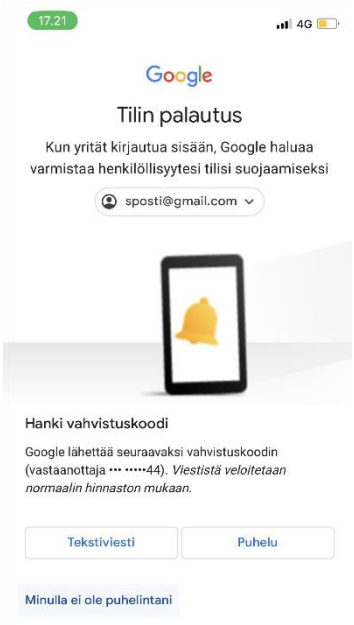
- **Nordea [Face ID & Touch ID]**



2. Benchmark, Nordea ID

  - Simple and clear usage
  - Fast login
  - Aesthetic design
  - Button for changing the authentication method

- **Gmail [Biometric authentication with number]**



3. Benchmark, Gmail

  - Simple and clear usage

    - Secure, since is only accessible with your number
    - Slower login
    - Account sharing without giving login details

- **Amazon [Voice ID]**
    - A bit complicated
    - Not as effective if there’s background noise
    - Voice tone can be faked
    - Not as fast nor secure

We have three main user groups: new users' group, security awareness group and efficiency group. New users don’t know how our product works, so they need easy and simple interface to get started. Nothing extra to confuse for great first interact with our product. For security awareness group it is important that using our product is safe to use. We must make sure that our product looks professional and of course has solid security. Efficiency group wants our product to run fast and smoothly. Response times must be fast and loading times as short as possible. We need to combine these needs together to make usable product for everyone.

User Survey

We made a survey of 10 questions to find out which login methods are the best and the most memorable. Target group for this survey is all regular smartphone users.
Our questionnaire is focused on finding the overall development, issued and status of password-free login systems. We want to map the combining factors of our identified user groups to see, which aspect of the system is the most relevant to the most users. We want to keep the questionnaire short to avoid fatigue as respondents could lose interest with multiple questions.

Questions:

1. What login method do you use to open your own phone?
2. What login methods have you used to log in to different apps? (e.g. password, facial recognition, fingerprint recognition...)
3. What is your preferred login method and why?
4. Which login method do you dislike and why?
5. Do you use the same password in multiple places?
6. In your opinion, what is the safest login method?
7. How would you rate the security of facial and fingerprint recognition as a login method?
8. Have you ever experienced security issues with any login method?
9. Is there a login method you would like to use, but it is not available?
10. What kinds of login methods would you like to see in the future?

2 UNDERSTAND

Contexts of use for already-in-use alternatives

App type	Organizational Context	Social Context	Physical Context
Banking apps	Banks are highly regulated and have a strong incentive to ensure that their apps are secure and protect customers' financial info	Managing money is a sensitive matter and users expect a high level of privacy and security when using these apps	Banking apps are often used on the go, such as when someone needs to quickly check their balance or transfer money while out and about
Social media apps	Social media companies have a strong incentive to offer two-factor authentication to protect users' accounts from hackers	Social media is a highly social activity, and users want to be able to share their thoughts and opinions with others	Social media apps are often used on mobile devices, which means that users can access them from anywhere, at any time
E-commerce apps	E-commerce companies handle large amounts of sensitive personal and financial data and have a strong incentive to protect it	Online shopping is now a norm, and users expect a high level of security and privacy when making purchases online	E-commerce apps are often used in a variety of settings, such as at home, at work, or on the go
Healthcare apps	Healthcare organizations are subject to strict regulations that require them to protect patients' medical information	Healthcare information is highly personal, and patients expect a high level of privacy and security when accessing their records	Healthcare apps are often used in a medical setting, but may also be used by patients at home
Password mgmt apps	Password management	Passwords are an essential part of	Password management apps

	companies are in the business of protecting their customers' passwords and personal information	modern life, and users want to be sure that their password manager itself is secure	are often used on mobile devices, which means that users can access them from anywhere, at any time

Both are typically available as options in a plethora of apps. Let’s look at contexts of use for some of these:

2.1 User research findings

Answers to questions:

1. The majority of users (around 80%) use some form of login method to unlock their phones, with the most popular being a PIN code or fingerprint recognition.

2. The most commonly used login methods when logging into different applications are passwords, followed by fingerprint and facial recognition.

3. The favorite login method among our group is fingerprint recognition, as it is quick and convenient.

4. The least favorite login method is typing in a password, as it can be cumbersome and difficult to remember.

5. About 60% of users admit to using the same password in multiple places, which can pose a security risk.

6. The group generally agrees that the safest login method is a combination of biometric authentication (such as fingerprint or facial recognition) and a strong password.

7. Facial and fingerprint recognition are generally seen as secure login methods, but there are concerns about the potential for false positives or hacking.

8. Several users have experienced security issues with their login methods, including password leaks and unauthorized access.

9. Some users expressed interest in using voice recognition as a login method, but it is not currently widely available.

10. Future login methods that our group would like to see include more advanced biometric authentication, such as retina or vein recognition, and more seamless integration with wearable technology.

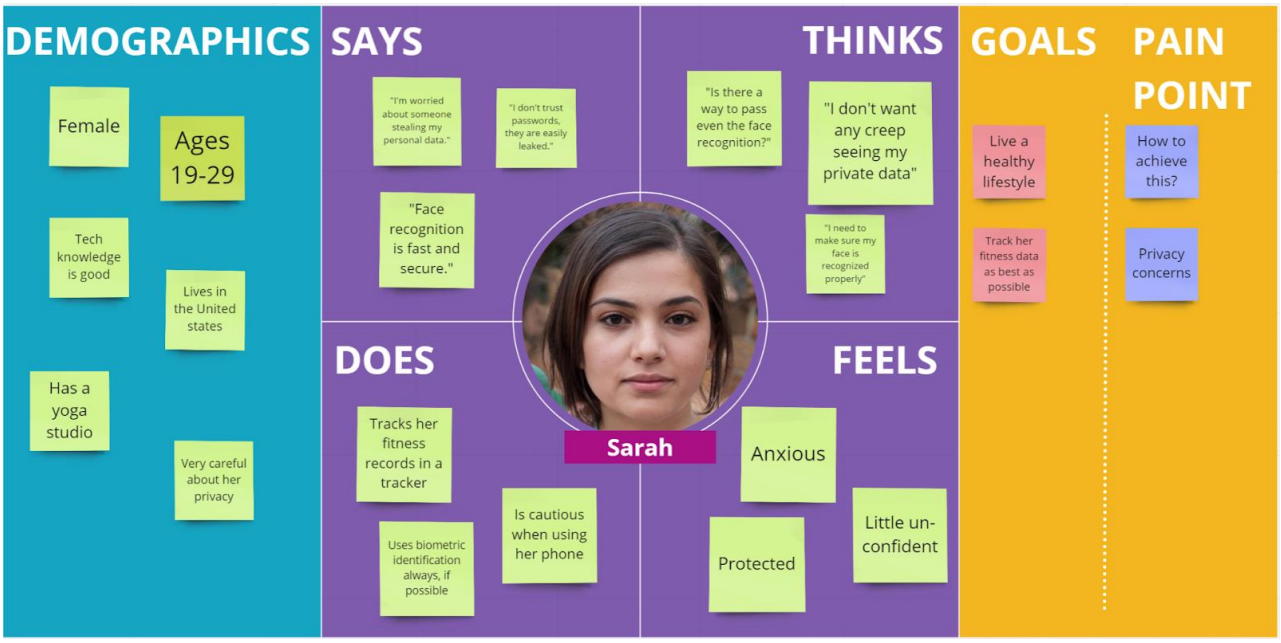
Summary: “Visualizing user attitudes and behaviors in an empathy map helps UX teams align on a deep understanding of end users. The mapping process also reveals any holes in existing user data.” (Gibbson, 2018).
In other words, an empathy map is a tool that helps teams understand how users feel and behave. By using this tool, user experience (UX) teams can get a better understanding of their users. This process also helps identify any missing information about the users.

Let’s look at a couple of different users and their empathy maps:

John: John is a busy businessman who uses biometric identification on his mobile device to quickly access his phone without having to type in a passcode. He prefers to use the fingerprint scanner as it is convenient and reliable.

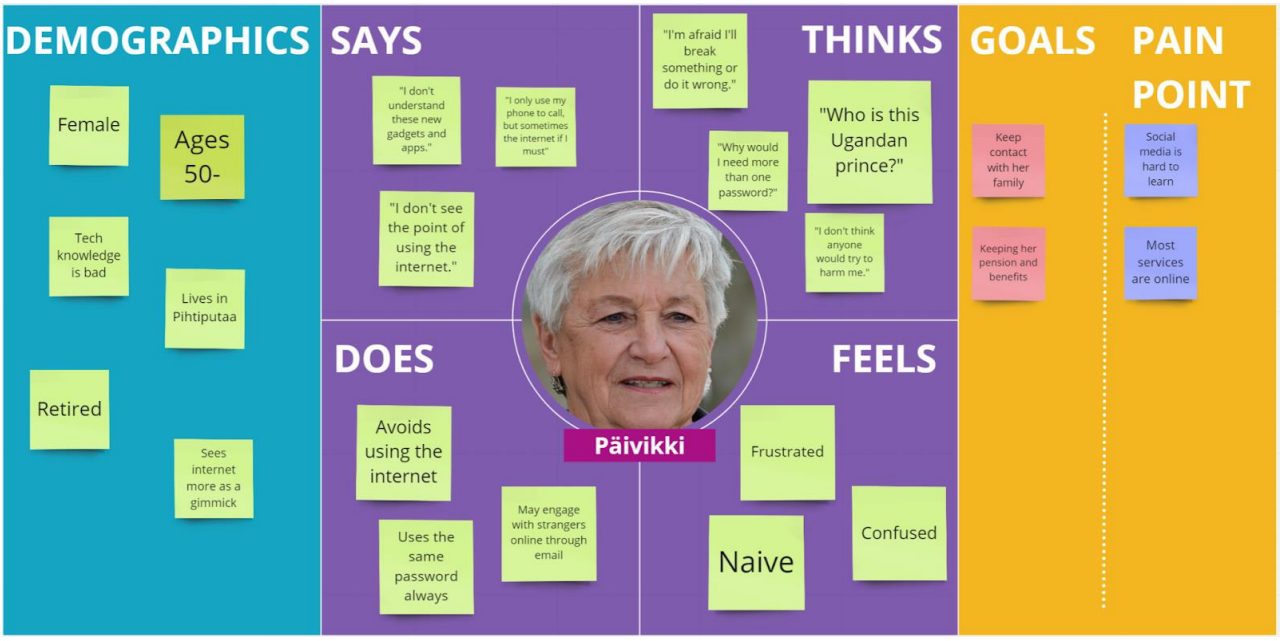
4. Demographic, John

Sarah is a fitness enthusiast who uses biometric identification on her mobile device to keep her personal health data secure. She uses the face recognition feature to ensure that only she can access her fitness apps and track her progress.



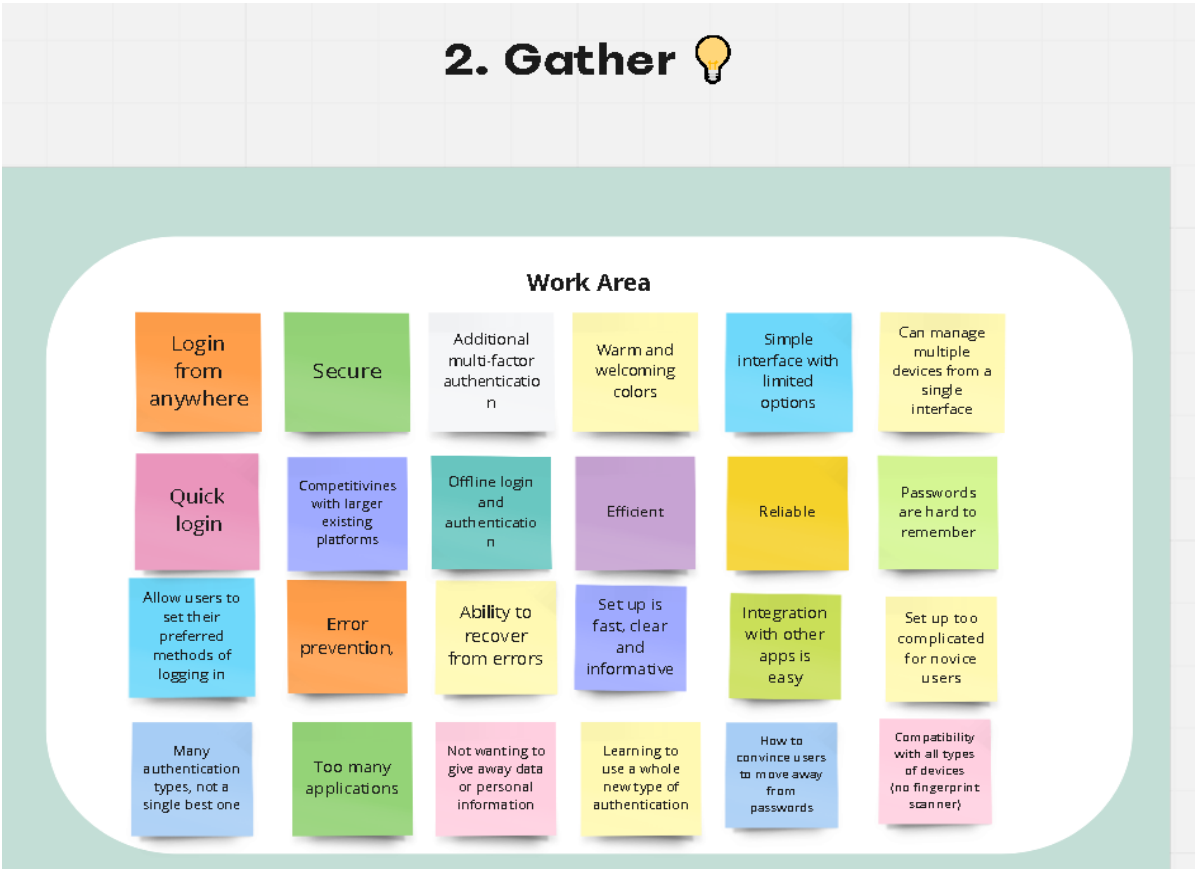
5. Demographic, Sarah

Päivikki is an elderly woman unfamiliar with modern technology and its potential risks. She prefers to communicate with her loved ones through phone calls or in-person visits, and she is not interested in exploring the Internet. Despite her lack of knowledge about online safety, Päivikki may engage with strangers or unintentionally download malware.

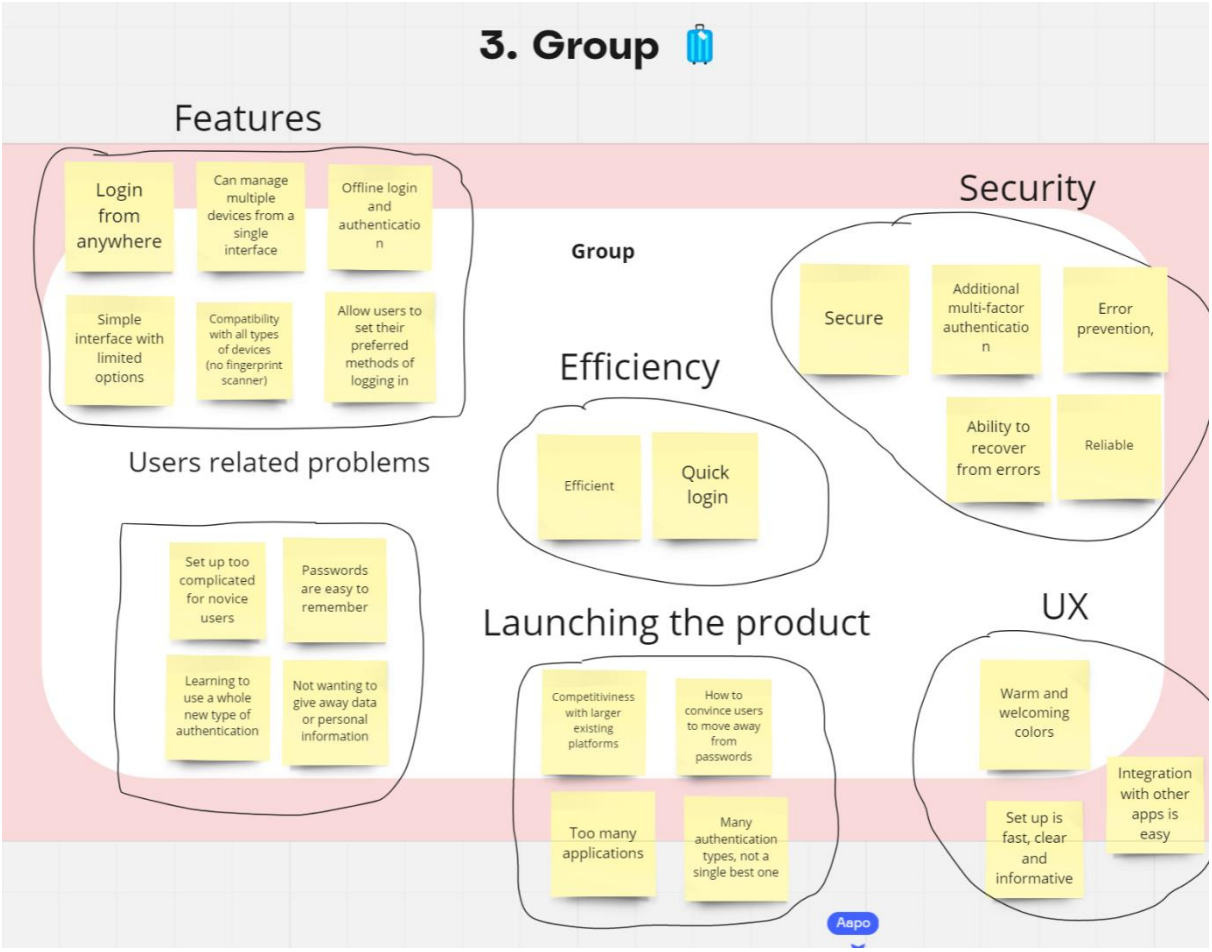


6. Demographic, Päivikki

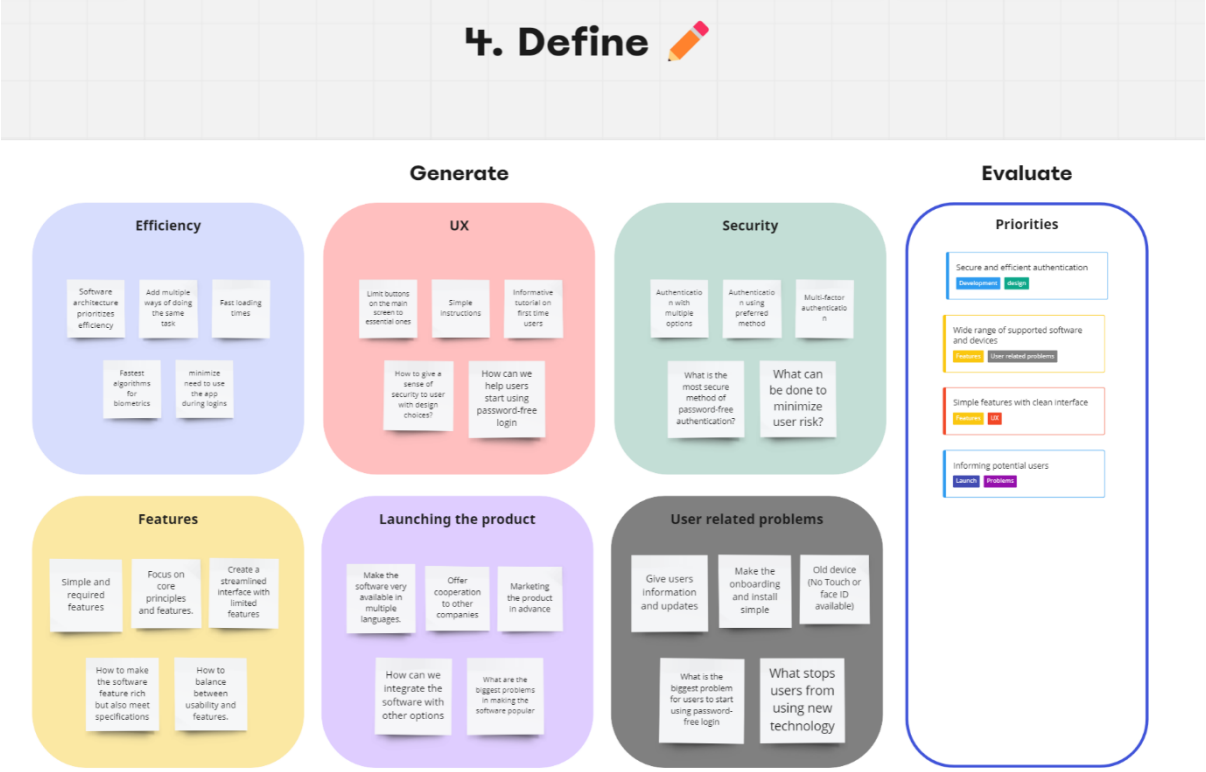
Affinity mapping



7. Affinity, Gather



8. Affinity, Group



9. Affinity, Define

Personas

Susie, 28, Online Shopper (Primary User)

Susie works as a marketing professional, and she spends a lot of money ordering clothes and technology online. For Susie it is important that her money stays safe, so she needs high security from authentication application. Interface must look professional and trustworthy to make Susie rely on it. Susie prefers to use biometric authentication methods, mainly fingerprint recognition. Also, long waiting times annoy her when she wants to complete every transaction as fast as possible.

Margaretha, 69, Retired World Traveler (Primary User)

Margaretha is wealthy thanks to her hard work in the past and huge corporation acquisition at the end of her career. She has travelled many years around the world after her working days. As an old business lady, she knows that she needs to take good care of her money and as she books flights and hotels her focus is always on safety. From authentication application she needs an easy enough interface and a lot of security to keep her money safe.

Anton, 23, CEO (Secondary User)

Anton owns a mobile game application and wants a secondary authentical method for a reliable login and secure way to enhance the login process. He does research for a trustworthy method and comes up with our application. Now he utilizes our application as one authentic method for login on his mobile game.

Central Bank of Uganda (Secondary User)

Central bank of Uganda (CBU) has faced some major security issues on its own authentication for mobile devices. They decided to contact us to temporarily use our application to log in to their bank accounts. This deal bank can keep their clients safe while they work on their own authentication to be secure.

3 DESIGN

3.1 Ideate

We used our benchmark research (Chapter 2) to determine the most common solutions for authentication systems. We grouped these together using personal opinions, user survey and the table (Appendix 1) provided by Bonneau et al (2012) based on most secure at the moment and most used at the moment. We then used the intertwining concepts to determine technologies that are already used and secure, meaning people already are adapting to their presence in everyday life. We then formed the most applicable category from which we could determine options that could offer potential solutions and enhancements to current technologies.

Most secure

Fingerprints

Retina scan

Implants and microchips

Physical cards and scanners

Most used

Password managers

Face ID or facial recognition

Bank ID

Multi-factor and phone based

Physical scanners

=> Most applicable

Face ID or facial recognition

Implants and microchips

Physical scanners

Multi-factor authentication

However, in the table (Appendix 1) provided by Bonneau et al (2012), we can determine that the options available currently are either deployable, secure or user-friendly but never all three. Thus, we've determined to prototype towards increasing the usability of already secure and deployable technologies, as that can be improved upon. We selected the following technologies for our possible solutions:

CAP Reader – Reads a SIM or authentication token from a physical object.
OTPW – One Time PassWord.
PassWindow – Key pattern printed on a physical card.
Face ID- Facial recognition.

Note that these technologies and others could be combined for a potentially more secure system, but the more authentication passes are required from the user, the less usable and linear the system becomes.

We decided on creating an authentication software that can be used to authenticate different applications or services on a centralized platform, while combining multiple log-in methods. Our initial prototype will have a facial recognition as the default case, as that is common and testable.

3.2 User Journey

For our user journey ideation, we decided to choose the most inexperienced with modern technology, Päivikki. Our goal is to make the interface and experience as simple and usable as possible, while still instilling a sense of security in the user. Our intended use case is for Päivikki to be able to log in to KELA services with their mobile device, while creating as little error in the process as possible and guiding her through the process if an error does occur.

Päivikki starts their interaction with our application by going to KELA authentication and selecting our application as their chosen method for logging in. Päivikki then gets asked a simple permission question to be moved to the application screen. Upon entering the application screen, it automatically detects which service Päivikki is logging into and takes into account their personalized options for authentication.

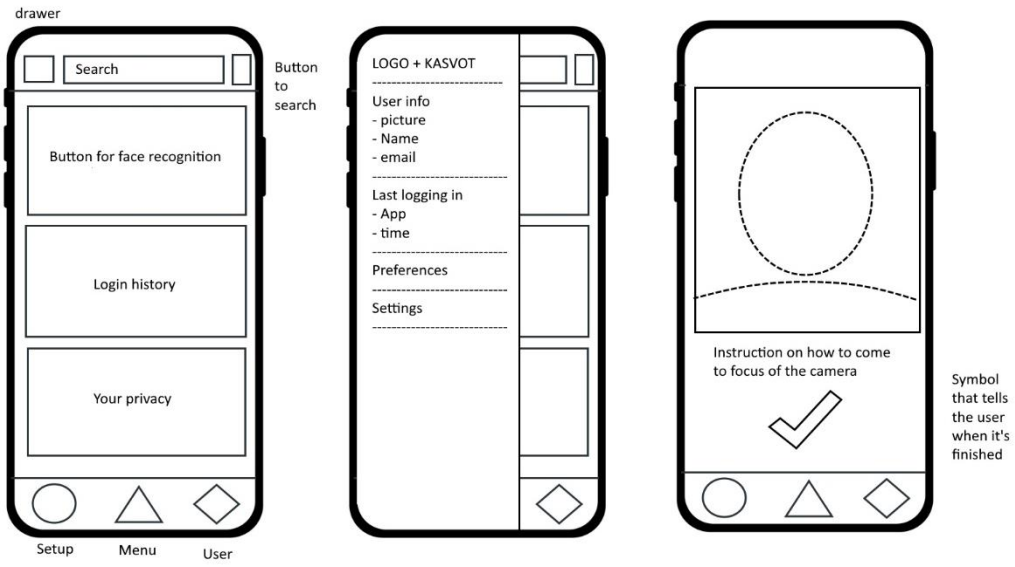
Päivikki's family has instructed her to look at the camera for facial recognition, so the software recognizes her and authenticates the request. If Päivikki is sitting a bit too far away from the camera or the interface cannot detect her, she is instructed in her selected language to complete the operation.

If facial recognition cannot be used, she is moved to further authentication steps, that her family has set for her. As the request completes, she is automatically moved to the KELA site and logged in, all in a fluent motion where she has to only give permission to be moved to the application screen. There should be a clear process for onboarding as well as in this case we expect Päivikki to have help in setting the system up.

3.3 Prototype

3.3.1 Part A: Paper prototype (hand drawn)

Our prototype will consist of three views: main, drawer and face recognition:



10. Paper prototype

The component layout and main design patterns are finalized in this prototype. The main view consists of a search bar, navigation drawer icon, card layout and a bottom navigation bar. Search bar allows the user to find information quickly. On the left side of the search bar there will be a navigational icon to open the app drawer and on the right a search button/icon.

The main view is mostly taken by the card layout which will consist of cards stacked on top of each other. These cards will contain a picture, titles to tell the user what their purpose is and buttons to navigate into the cards related actions. The visual hierarchy needs to be taken into consideration when building the card layouts. The main use cases of the app: face recognition, login history and your privacy will be placed here to be accessed quickly.

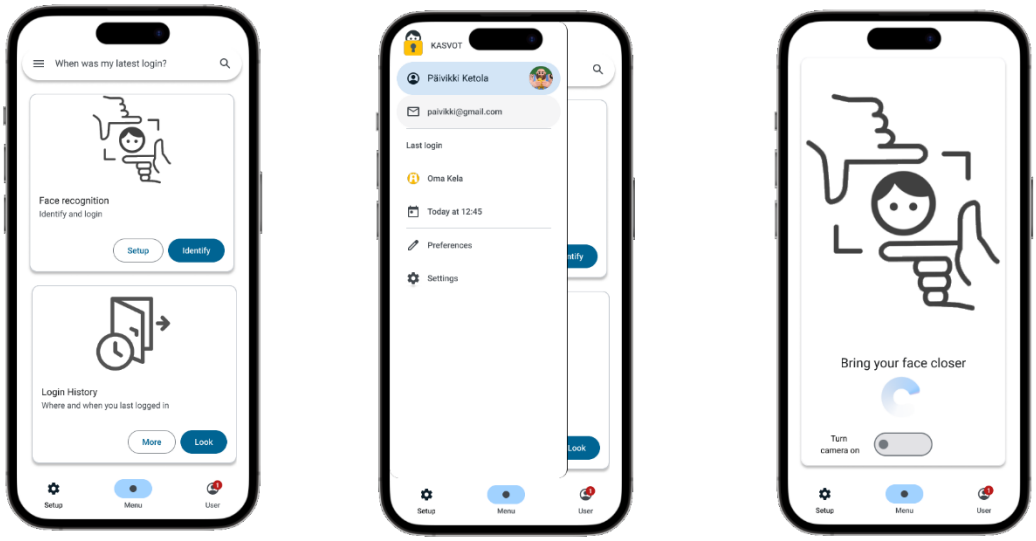
The bottom navigation bar will be visible on all of the views. It's the backbone to navigating our app. It will have the icons and text below to show the destination that they will take you to. The icon's color will change according to page the user currently on. The three most important destinations for our app will be menu, user and setup. Setup will be included

because the users preferred settings such as the preferred identification method will greatly affect the apps use.

The navigation drawer will provide access to rest of the destinations that the bottom drawer doesn't directly include. It will also show the users relevant current information and allow account switching. The items in the drawer will have clear icon and title to give the user a clear and familiar feel to the app. The different sections will be seperated with a divider line for a clearer grouping of items.

The face recognition will be a single card consisting of a logo or a view of the users face to show him the correct placement. Under it will be loading animation showing the current status of the identification. There will be a button to continue but there will be an option to continue immediately without confirmation.

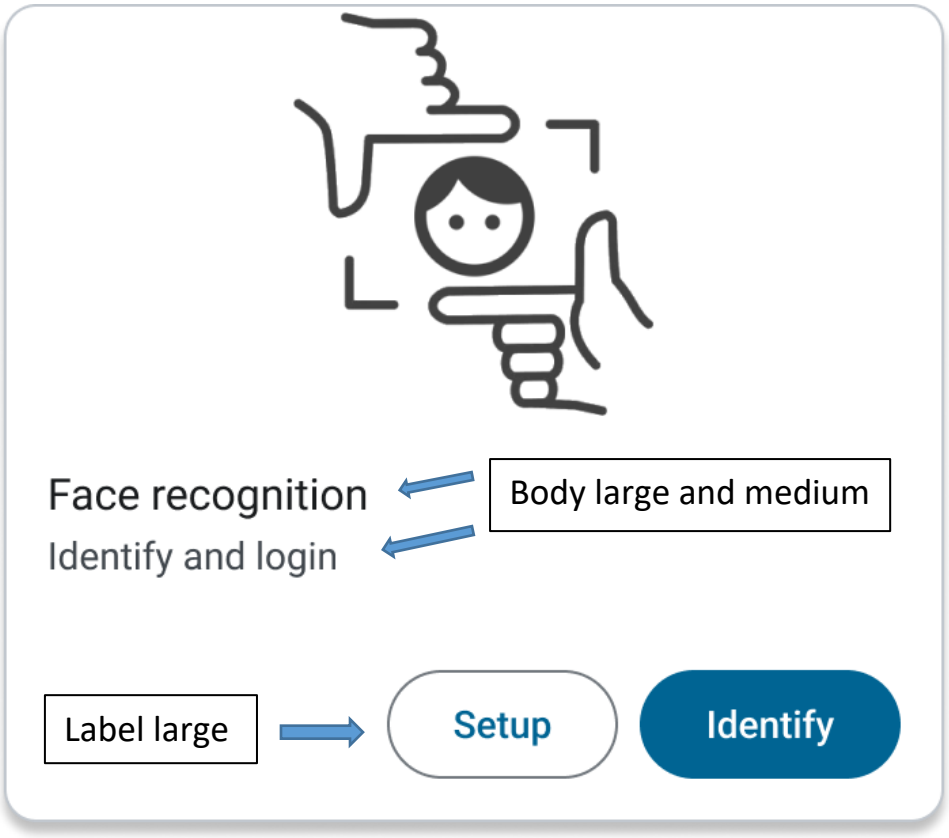
3.3.2 Part B: Digital prototype



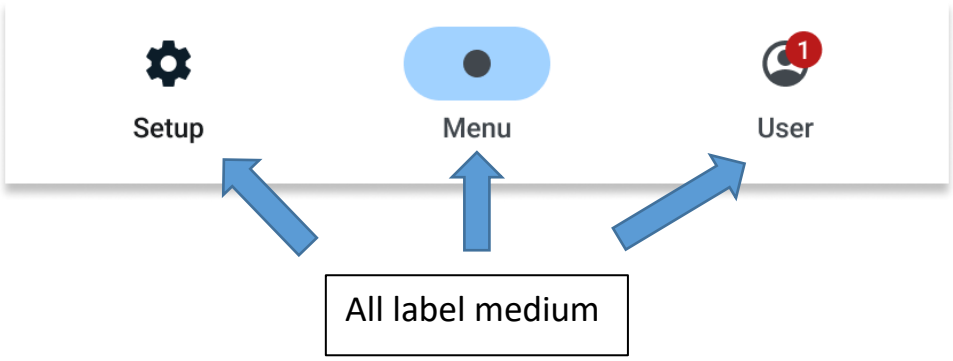
11. Digital prototype

Typography:

As a font we are using the android default Roboto. It has a very pleasing look that is very familiar to most of us. We are using the five type styles of materials three pack: Display, headline, title, body and label, to keep the style consistent. These five will then still extend to small, medium and large sizes, giving a total of fifteen unique text sizes.



12. Overview of material design



13. Material design navbar

Iconography:

We mostly combine the used icons with our typography to generate a cohesive style that is familiar and functional. The icon's main purpose is to symbolize common tasks and actions to enhance the learnability and the match of the app and real world.

We have used material packages own provided icons. These are a good mix of already familiarized icons that almost anyone can recognize. We chose the bold-filled variants of

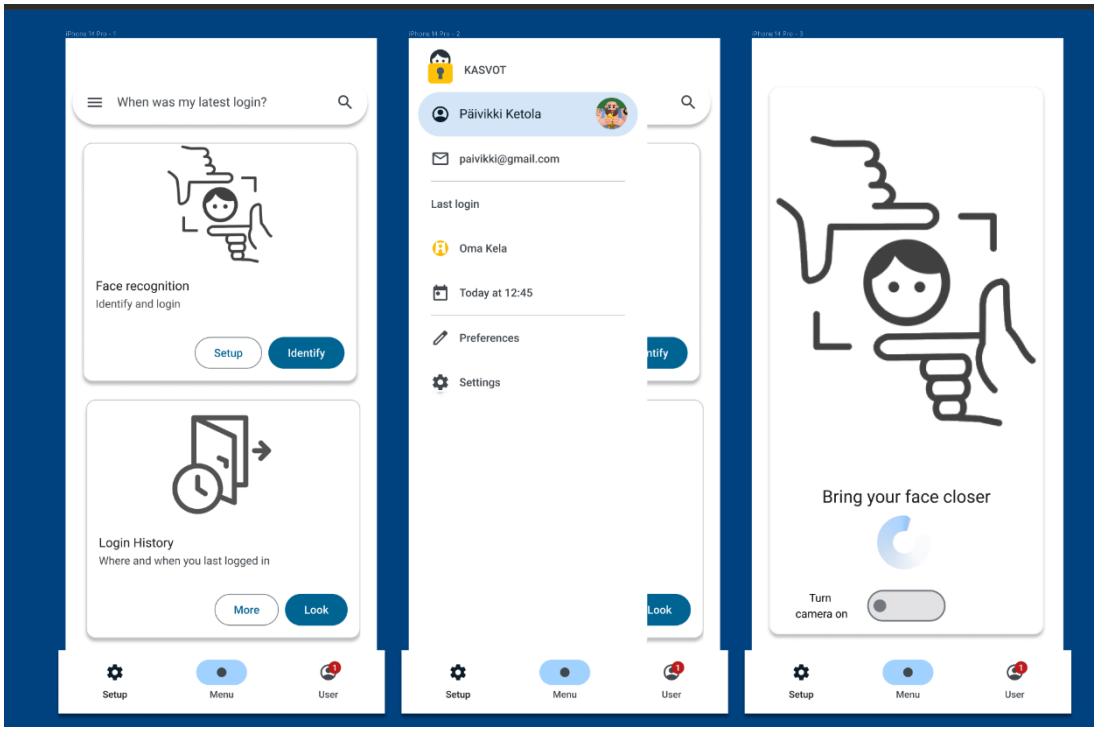
the icons to give more contrast to our mostly white interface.

We also made our own icons for the cards and logo. They all use the provided face icon with other outside assets. In our opinion this gives a unique and consistent art style across the app.

14. Logo ideation

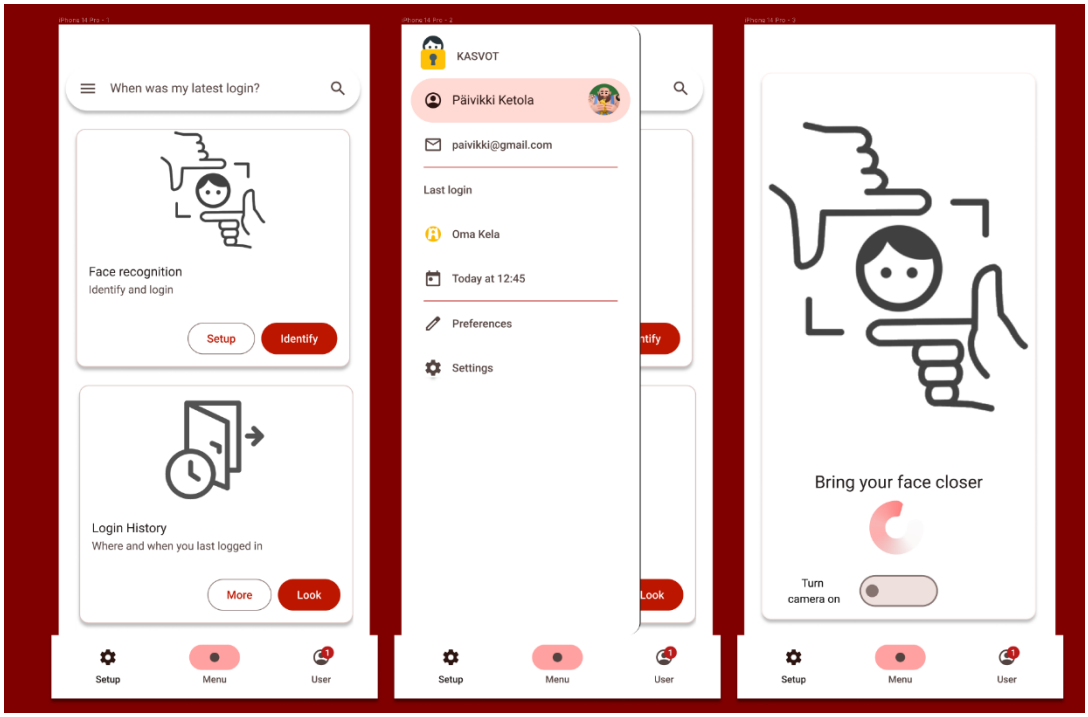
15. Color palette

The color palette at the end was between two primary colors: a Dark blue and a deep red.



16. Color palette: Blue

Dark blue is often used in UI design as a color that conveys a sense of professionalism, trustworthiness, and authority. It can also be used to create a sense of depth and contrast, particularly when combined with lighter shades of blue or other complementary colors.



17. Color palette: Red

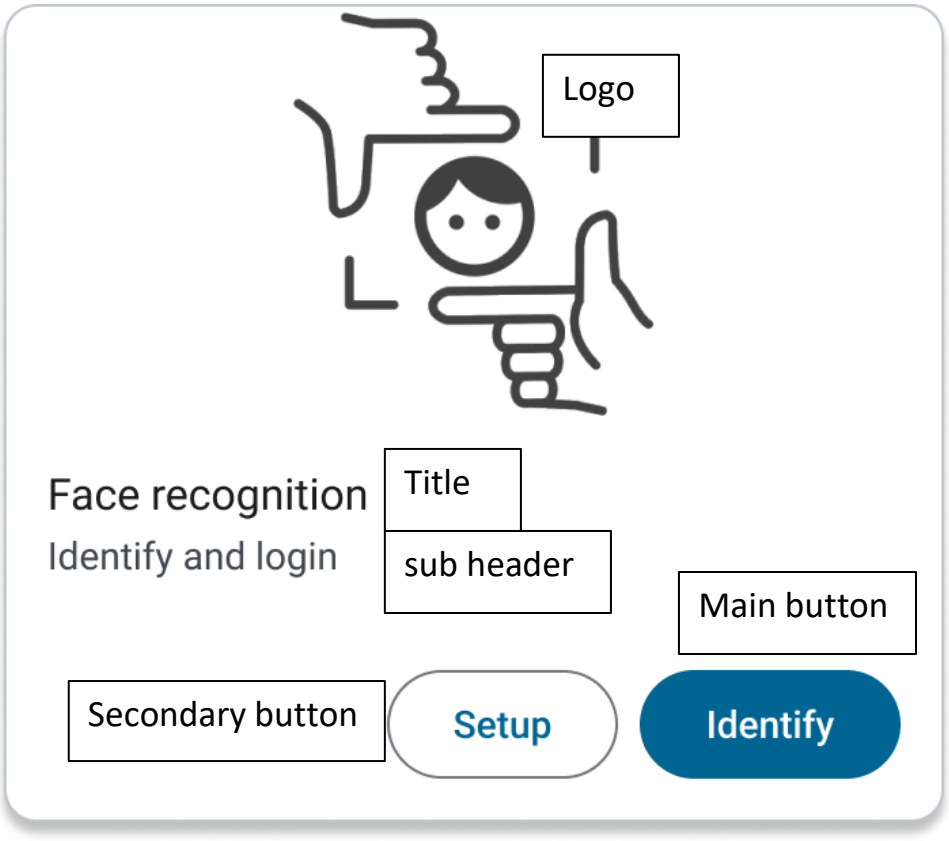
Deep red is a bold and attention-grabbing color often used in UI design to convey a sense of urgency, importance, or passion. It can be used to draw the user's attention to important buttons, notifications, or calls to action, and can also create a sense of warmth or intensity.

At the end we decided to save this decision to the usability survey and let the people decide.

Final components:

The main menu mostly consists of the card layout so the cards themselves received attention to make them the clearest they could be. This was done with a clear hierarchy between the components of the card. The cards largest item, the logo, is on top of the hierarchy for a reason. It gives the user the first impression of the task it does.

Next comes the title that tells the user clearly what the cards task is. Then come the buttons, they are colored in the order of their importance. And at last, the sub header tells the user more clearly what the cards purpose is.



18. Focused analysis on key features

The overall appearance of the app follows the patterns. Cards are little elevated and consist of one or two buttons near the bottom. All corners are rounded with the search bar and current user Identicator being completely rounded.

3.4 Heuristic evaluation findings

We only got two heuristic evaluations, where only one was good enough to even take into consideration, which made our job extremely difficult. But we still utilized the one evaluation with the best possible way and did some modifications to the first prototype.

The authentication application has a well-built and intuitive user interface that is easy to understand and navigate. The design is minimalistic and flexible, making it recognizable and familiar to users. The system's navigations are clear, aided using colours and simple buttons, and the structure remains consistent across different views.

However, there are some areas that need further explanation to enhance the user experience. For example, the purpose of the search bar and information on the side bar needs clarification. Some titles break the consistency, and there are minor inconsistencies that could be improved.

The system's learnability is okay, but there is room for improvement. The effectiveness of the system could be enhanced by making the face recognition screen easily accessible from anywhere in the app, not just home screen. The style feels overly strict and corporate, and adding a bit of personality could make the system more engaging.

3.5 Questionnaire feedback

We collected feedback from the digital usability fair with a survey presented in Appendix 2. We deliberately made the questionnaire open ended and long, since it was our only opportunity to gather feedback before getting graded.

On the survey itself, respondents deemed it to be very long and cumbersome to fill which resulted in us getting less than a desirable number of answers. We intentionally put each section as non-mandatory so that people could answer for as long as they felt comfortable with and then submit towards the end of their patience.

Some questions were also skipped, which showed that respondents were aware that they could skip questions. We wanted the data to show where respondents grew tired of answering but with a small sample size it is uncertain. The respondents overall felt that the questionnaire should be more concise and focus on a more specific aspect of the UI instead of the overall feel and fluidity of it. We also included too many questions where the users themselves had to come up with free form answers which resulted in tiredness.

As such, we expected to see a decrease in the responses towards the later portion of the questionnaire as opposed to people not bothering in the first place. We received a few quality answers from respondents but also a few AI generated, copy-pasted ones which we were very disappointed to receive. This led to use doubting the overall feedback given, as we could not be sure if the answer was AI generated or not. We nonetheless also received quality answers with explanations that we can use to further develop the prototype.

3.6 Questionnaire results

We had an initial idea of 3 key areas where we placed our main focus for the usability testing. These were Security, Simplicity and Features. We thought these 3 main topics would allow us to group ideas for the core usability instead of spreading our attention too thin on developing towards the backend functionality, instead of the user experience.

Security

On security, we focused on questions about the overall idea of password-free login as that is a key focus in finding a suitable opening for our application to differentiate itself from the competition. The respondents seemed wary about using a centralized platform for authentication and believed the facial recognition to not be as safe as other options could be. Respondents also felt like the solvable problem in terms of security was either developing a more robust authentication service, not necessarily the user interface.

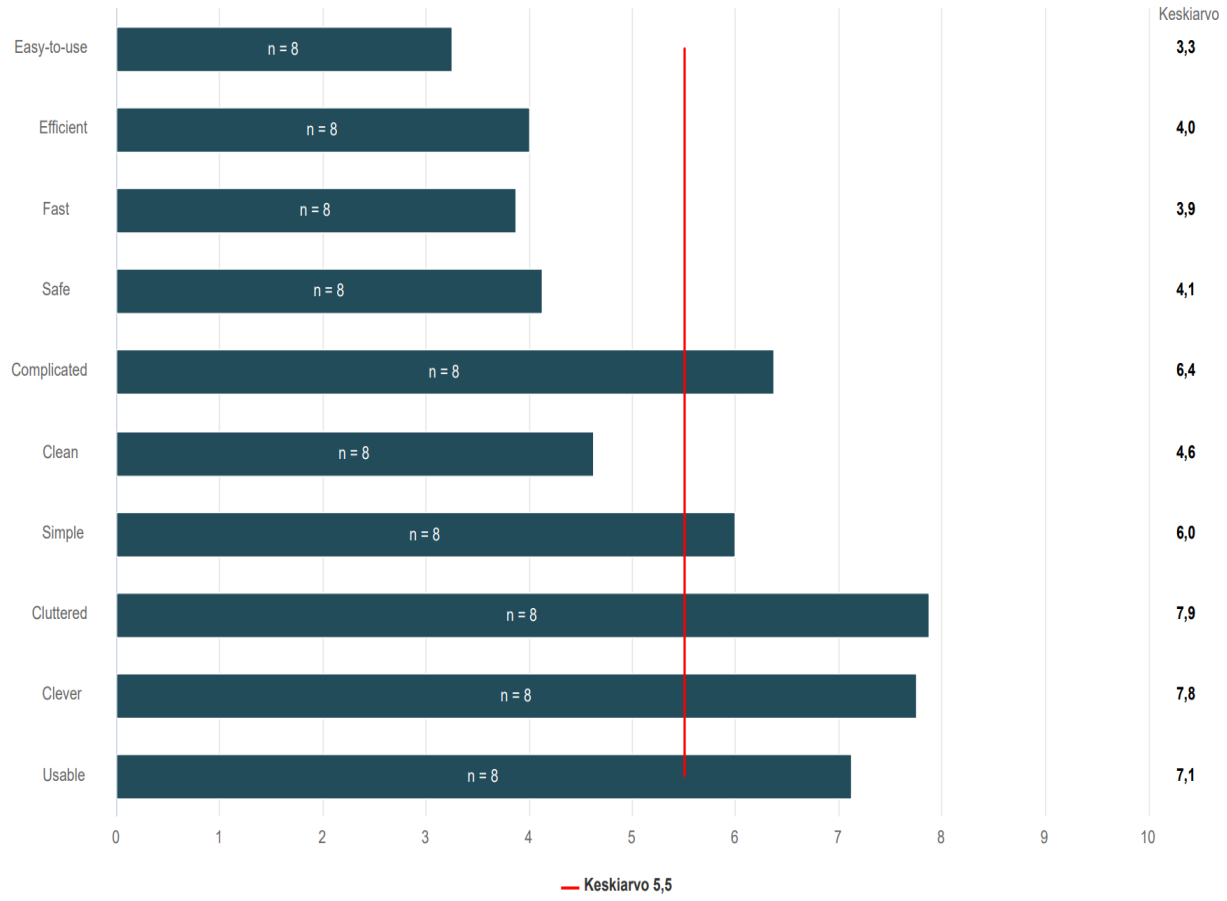
Simplicity

We want to provide an application that is designed to be used for the most inexperienced user of password-free logins and services. As such the survey included questions on ease of navigation, use cases, resemblance to other applications and security. Respondents felt like the interface was simple and minimal with efficient navigation. We however received feedback that the user interface was not outstanding and similar to other corporate solutions, making it blend in a bit too well. They also included a point about having a search bar which had no purpose in their minds.

Features

For features, we decided on asking questions about the necessary features and features respondents felt like were essential to the experience. One respondent felt like the face recognition should be the main focus on the screen and someone suggested we should remove the search bar in an effort to further simplify the interface. We also asked if the respondents would prefer different colour palettes, with a skyblue variant winning out by a majority.

We thought the well thought out answers and responses gave us tangible ideas we could implement into our final prototype. Our survey could’ve been more concise and focused on a more key set of issues.

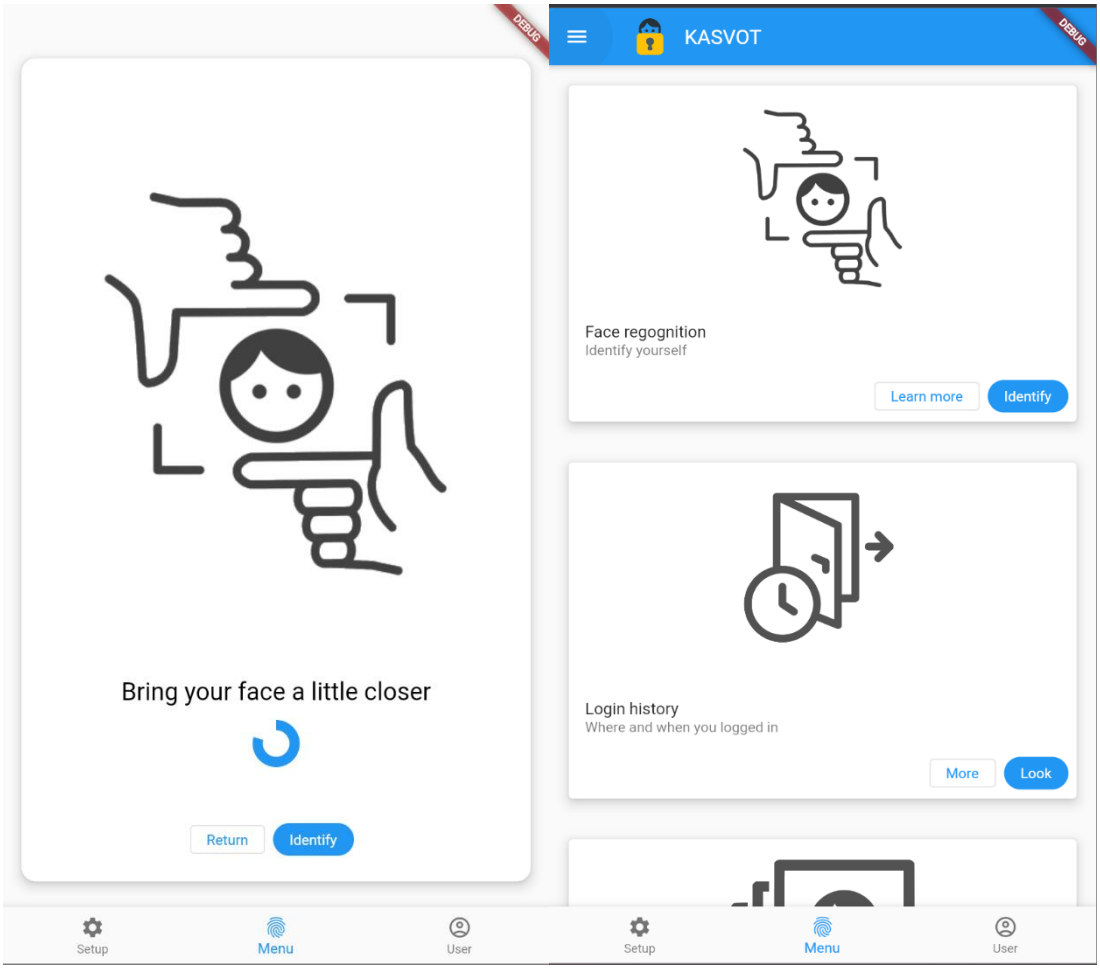


19. Questionnaire term association table

As pictured in Figure 19, we also included a term association chart to map the overall feeling people had for the app. A rank of 1 would be the term most associated and rank of 10 would be the least associated. We hoped to gain a favourable (under 5) grade in Ease-of-use, efficiency, cleanliness and simplicity above the others. We accomplished a part of those goals, but the term association task in particular was challenging and cumbersome to respondents.

4 PRODUCE

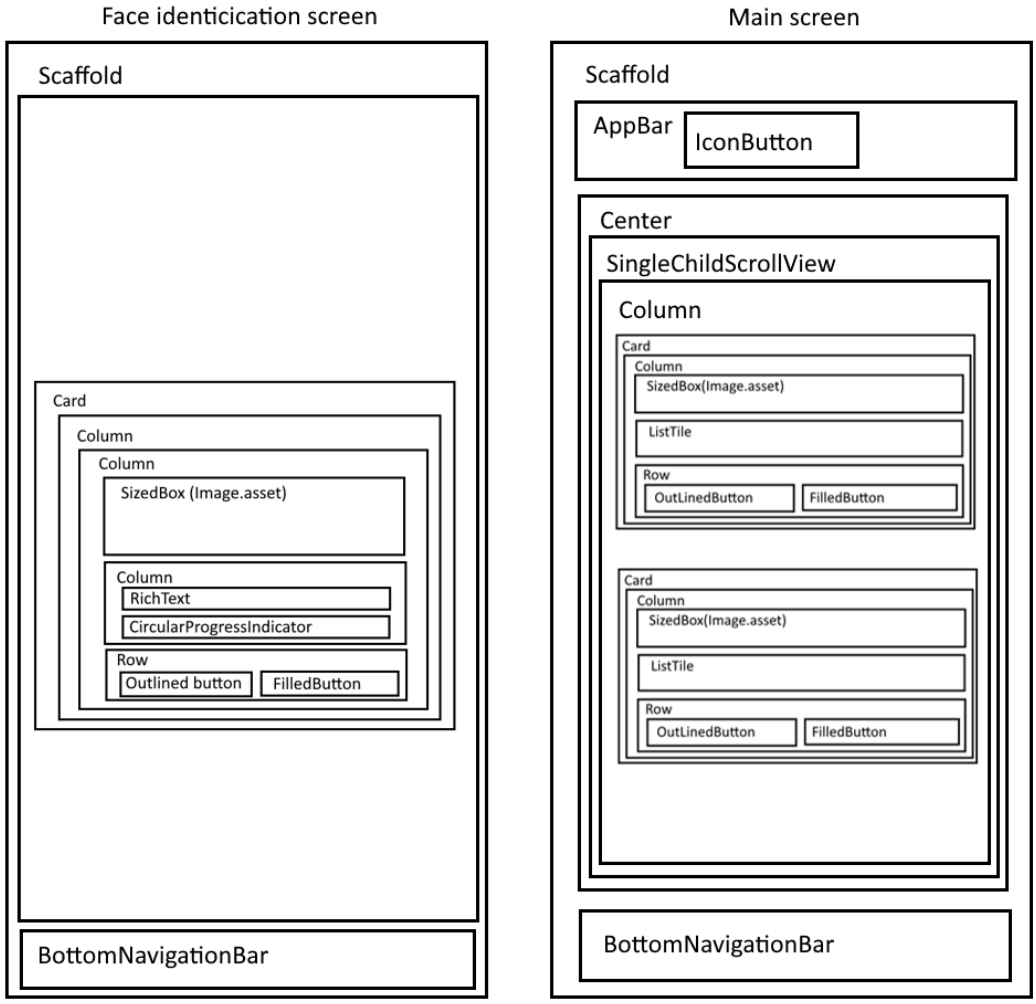
From the heuristic evaluations and questionnaire, we gathered the feedback and decided that a separate search bar was unnecessary. Also, the option to look at the services you sign into using our app came up and was decided that it would be replacing the information card about your privacy. The face recognition view also didn't have a separate cancel button so that was added. Dark blue won by a land slide and will be the color theme for the final prototype.



20. Final prototype

The material design choices remained mostly the same (refer 3.3.1).

The image below shows a simplified view of the builds. They show the main widgets used in and how they are layered.



21. Final prototype layout scheme

Impractical parts of the design was the navigation drawer. It could have been made but due to time constraints it was never implemented. Also the bottom drawer and the navigation overall isn't quite what the figma prototype had but could be implemented with more time given.

The main widget both builds use is Scaffold widget that's a good starting point. It gives the option to add the BottomNavigationBar painlessly. Both Column and Row widgets were all used extensively throughout the app to align the buttons and items correctly. The Card widget was used to make the card components. Different buttons such as OutlinedButton and Filled button were used to match the prototype.

Responsive design was not implemented to the final prototype but the card view would have gone from a stacked layout to a layout where cards also go horizontally.

REFERENCES

1. Zhu, B., Xinxin, F., Guang, G. 2014. Loxin- A Universal Solution to Password-Free Login [article] [Referenced: 1.4.2023] Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=28abb62f15e5913839314deefe1f18c8166299a0
2. Bonneau, J. Herley, C., van Oorschot, P., Stajano, F. 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. [article] [Referenced 1.4.2023] Available: https://www.cl.cam.ac.uk/~fms27/papers/2012-BonneauHerOorSta-password--oakland.pdf
3. Gibbson, S. 2018 Empathy mapping: The first step in design thinking, Nielsen Norman Group. [article] [Referenced 7.4.2023] Available at: https://www.nngroup.com/articles/empathy-mapping/

APPENDIXES

APPENDIX 1. Password-Free Login method evaluation

Category	Scheme	Described in section	Reference
(Incumbent)	Web passwords	III	[13]
Password managers	Firefox	IV-A	[22]
	LastPass		[42]
Proxy	URRSA	IV-B	[5]
	Impostor		[23]
Federated	OpenID	IV-C	[27]
	Microsoft Passport		[43]
	Facebook Connect		[44]
	BrowserID		[45]
	OTP over email		[46]
Graphical	PCCP	IV-D	[7]
	PassGo		[47]
Cognitive	GrIDsure (original)	IV-E	[30]
	Weinshall		[48]
	Hopper Blum		[49]
	Word Association		[50]
Paper tokens	OTPW	IV-F	[33]
	S/KEY		[32]
	PIN+TAN		[51]
Visual crypto	PassWindow		[52]
Hardware tokens	RSA SecurID	IV-G	[34]
	YubiKey		[53]
	IronKey		[54]
	CAP reader		[55]
	Pico		[8]
Phone-based	Phoolproof	IV-H	[36]
	Cronto		[56]
	MP-Auth		[6]
	OTP over SMS		
	Google 2-Step		[57]
Biometric	Fingerprint	IV-I	[38]
	Iris		[39]
	Voice		[40]
Recovery	Personal knowledge		[58]
	Preference-based		[59]
	Social re-auth.		[60]

●= offers the benefit; ⭘= almost offers the benefit; *no circle* = does not offer the benefit.
▥= better than passwords; ▤= worse than passwords; *no background pattern* = no change.
We group related schemes into categories. For space reasons, in the present paper we describe at most one representative scheme per category; the companion technical report [1] discusses all schemes listed.

Table I
COMPARATIVE EVALUATION OF THE VARIOUS SCHEMES WE EXAMINED

Appendix 1. Evaluations of different methods of authentication (Bonneau et al. 2012).

APPENDIX 2. Usability questionnaire

What security option or options would you like to use for a password-free login system?

Do you think the idea is viable?

If not, can you describe the biggest issues you find with password-free logins?

Would you like an alternative to your current login options?

Would you use a centralized authentication platform for multiple services?

Which adjectives would you use to describe the current state of the user interface?

Is there a feature you would add or that you think should be added to the interface?

Is there a feature that you think does not make sense?

Is there a feature that you would not use or see as clutter?

Is there anything the app resembles?

How do you expect the finished version of application to work? Describe it as a process shortly.

When using facial recognition, would you prefer seeing your face or not?

Does the placement of features make sense? Can you find all of the features you would expect?

Can you navigate the application efficiently?

Describe a use case the application could have

Here are two versions of the user interface with varying colours, which palette would you prefer?

Here are two logo ideas for the app, which would you prefer?

Rate the application on how you feel about it in these categories from 1-5

Easy-to-use
Efficient
Fast
Complicated
Safe
Clever
Cluttered
Usable
Clean
Simple

Give us open feedback on questionnaire:

Give us open feedback on user interface: