MinID Prototypes

Brage Asperanden Navarsete
Institutt for informatikk
Kristiania
Bergen, Norway
Brage.Asperanden.Navarsete@digdir.no

Eiril Solveig Ugulen
Institutt for datateknologi og informatikk (IDI)
NTNU
Trondheim, Norway
mailto: Eiril.Solveig.Ugulen@digdir.no

Audun Kristian Oklevik
Institutt for informatikk
Universitetet i Bergen
Bergen, Norway
Audun.Kristian.Oklevik@digdir.no

Andreas Conradi Nitschke
Institutt for Ingeniør- og teknologiutdanning
Høgskulen på Vestlandet
Bergen, Norway
Andreas.conradi.nitschke@digdir.no

Kristoffer Svedal
Institutt for datateknologi og informatikk (IDI)
NTNU
Trondheim, Norway
kristoffer.svedal@digdir.no

Thea Ueland
Institutt for informatikk (IFI)
Norges arktiske universitet (UiT)
Tromsø, Norway
tue001@uit.no

Kae Saito
Institutt for Teknologi og Innovasjon)
Høyskolen Kristiania
Oslo, Norway
kae.saito@digdir.no

Kristian Gullhaug Birkeli
Institutt for data- og elektroteknologi)
Universitetet i Stavanger
Stavanger, Norway
kristian.birkeli@digdir.no

***Abstract*—This paper presents the MINID-Mockups project, aimed at improving the design and the user flow for the MinID login. MINID is a government service that allows users to log in securely to various public services. The project's main goal is to improve the user experience and security by implementing a new login flow and two-factor authentication mechanism. This paper outlines the related work, architecture, design, implementation, and evaluation of the MINID-Mockups solutions.**

I. Introduction

The MINID-Mockups project endeavors to enhance the user experience and strengthen the security in the login process of the MinID platform. In response to the current interface's perceived outdatedness and usability challenges, the project group has developed three prototypes, each featuring innovative designs and improved user flows. By focusing on creating a more intuitive login process, the project seeks to attract greater user engagement and satisfaction. Additionally, the modernization of the MinID solution holds the promise of long-term sustainability, addressing the challenges posed by outdated systems and mitigating the costs associated with one-time code distribution. This paper presents an exploration of the project's objectives, methodologies, results, and the profound benefits of modernizing the MinID platform.

II. Related Work

User authentication and access control are critical components in digital government platforms, ensuring secure and reliable access to sensitive information and services. Prior research and solutions in this domain have explored various methods to enhance user login flows and implement robust security measures.

In the realm of user authentication, traditional username-password systems have been widely used, but they are susceptible to security breaches due to password vulnerabilities. To address this, two-factor authentication (2FA) has gained prominence. 2FA requires users to provide two forms of identification, such as a password and a one-time code generated on a mobile device, adding an extra layer of security.

III. Description

The primary scope of the MinID-Mockups project was to create prototypes and examples of how the login flows could be improved in a final solution, with a focus on enhancing the user experience and strengthening security. Currently, there are two login methods, both utilizing 2-factor authentication (2FA). The first method involves entering a personal ID number and a password. After providing this information, the user clicks the "next" button to receive a one-time code(OTC) on their phone. Upon entering the received code, the user is successfully logged in. The second method follows a similar process to the first one. The user enters their personal ID number and password, but instead of receiving a one-time code on their phone, they receive a notification on the already downloaded MinID app. The notification requests the user to accept the login, and upon acceptance, the user is successfully logged in. The current MinID interface is perceived as outdated and not very user-friendly. Furthermore, another challenge arises from the cost associated with sending one-time codes to users, especially when a majority of users rely on the one-time code (OTC) methods. The expense of this approach can become costly over time. The modernization of the MinID solution presents a multitude of advantages, with a profound impact on user satisfaction. Modernizing the MinID solution offers numerous benefits. Enhancing the design and user flow can significantly boost user satisfaction. By implementing a more intuitive design and streamlining the login process, MinID, as an electronic ID, can attract greater user engagement and interaction. Another benefit with modernizing the solution is sustainability, outdated systems may become more challenging and costly to maintain and support over time. Modernization ensures the platform's long-term sustainability, reducing maintenance efforts and facilitating future updates and improvements. The project group has developed three prototypes with new designs, focusing on both interface and user flow enhancements. The decision to create three prototypes with new designs was driven by the desire to offer the MinID team a range of solutions to consider. By presenting multiple prototypes, the team can gain insights and inspiration from different design approaches, leading to a more comprehensive evaluation process. This approach allows for a broader exploration of potential improvements, ensuring that the final solution benefits from the strengths of multiple designs rather than relying solely on one concept. When creating new flows, the project group encountered the challenge that the more user-friendly the flow became, the less secure the solution was at the expense of security.

IV. Architecture

In the project, you will find different implementations of the design organized into separate folders. The first implementation represents the original design, the second implementation showcases the optimized design, and the third implementation features the original design with a different color scheme and layout. Each design has its own root directory within the implementation folders. To run all the different designs within the project, npm is used to install the necessary dependencies and build the extension. Run npm install in all the folders to install the required dependencies. See the setup section below for more information.

Following is the file structures (in order) for implementation 1, 2, and 3.

V. Design

The design section delves into the technical details of the MINID-Mockups solution. It outlines the data schema and database structure used to store user information securely.

A. Implementation 1 and 3 user flow

In the login flow of Implementation 1, the user begins by entering their personal ID number. The system then checks if a user account has already been created with the provided ID number. If a user account exists, they proceed with the

Figure 1. This is the file structure

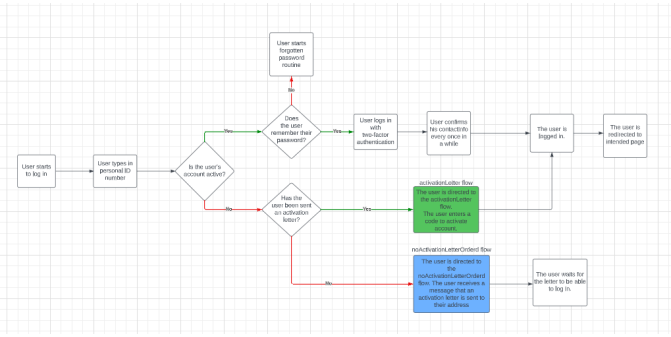

Figure 2. Flow 1 and 3

standard login process. However, if no user account is found, the user is directed to a new page. From this new page, users are presented with two different paths based on their previous actions. If the user has already ordered an activation letter, they will proceed to the ”Register the code on the activation letter” section. Here, they can register their password and contact information for future use. On the other hand, if the user hasn't ordered an activation letter, they will be redirected to the ”Order activation letter” page, where they can easily request and receive an activation letter. By providing distinct paths for existing users, users with an activation letter, and users without an activation letter, Implementation 1 aims to streamline the login process and ensure a smooth and personalized experience for each user.

B. Implementation 2 user flow

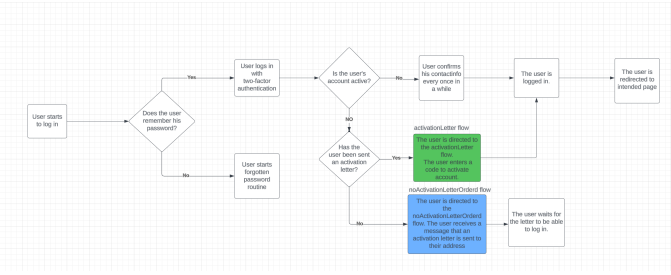

Figure 3. Flow 2

In Implementation 2, the login or registration process begins with the user using the MinID app. The user can access the app by logging in with their personal ID number and password or by registering their user in the app if they haven't already done so.

Once in the webpage, the user is presented with a QR code that they can scan using the app's built-in QR code scanner. After scanning the QR code, the user is prompted to enter their password. Upon entering the password, the user is successfully logged in to their account.

However, if for any reason the user is unable to use the QR code scanner in the app, they have an alternative option. They can click on the ”Use One-Time Code” button, so that the user can use a generated one-time code within the MinID app. Upon receiving the one-time code, the user can then proceed to the login page on the web browser.

At the login page, the system verifies which personal ID number the one-time code belongs to. The user is then prompted to enter their password. Once the password is entered, the user is successfully logged in to their account.

In both cases, the QR code or the one-time code serves as a secure and convenient method to initiate the login process, offering users flexibility and ease of access to the MinID platform.

VI. Implementation

In this chapter, we present the implementation of the three developed solutions aimed at improving user authentication and access control in the MinID platform. It covers technical aspects, design choices, and the integration of two-factor authentication, offering insights into the innovations introduced in the MINID-Mockups project.

A. Implementation I

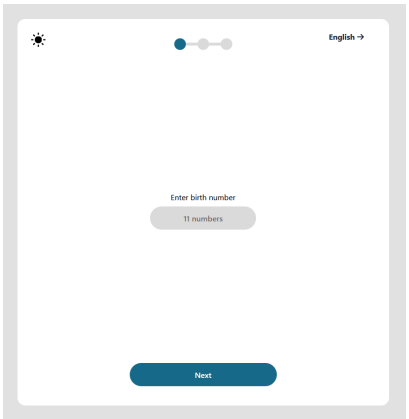

Figure 4. Implementation I

This design uses the birth number first to make the login process easier for the user. However, this solution is not very secure because of the risk of sanitizing national identification numbers. Due to security concerns, this design requires further research before being deemed suitable for implementation.

As a result, we do not recommend proceeding with this implementation at this stage.

The design features a clean and minimalistic interface with a blue and white color scheme. The login screen is uncluttered, displaying only essential information to the user. It adopts a user-friendly approach with a focus on simplicity. The birth number entry field takes the center stage, making the login process straightforward for the user. However, the security of this implementation is a concern due to the risk of sanitizing national identification numbers. As a result, further research is required before considering its implementation.

B. Implementation II

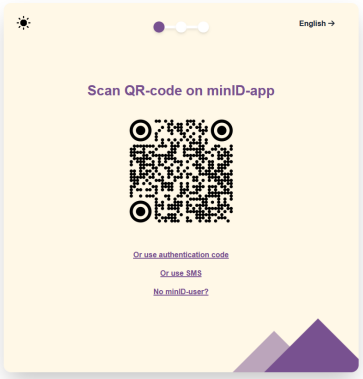

Figure 5. Implementation II

This design incorporates a QR code to enhance the user's login experience. The QR code is generated by the MinID app, allowing users to conveniently log in by scanning it. This solution is highly advantageous as it strikes a balance between security and user-friendliness. Although the SMS login buttons remain available, they have been downsized to encourage QR code usage. This approach not only reduces costs for the government but also enhances user security. The app will be linked to the user's national identification number, enabling swift login procedures. Upon scanning the QR code, the app provides login options through biometrics or by generating a 5-letter code for manual input. It's worth noting that this code remains active for a specific duration, ensuring both robust security and expeditious login processes.

The design exhibits a visually appealing design with a beige background and purple buttons. The login screen includes an eye-catching purple mountain illustration in the bottom right corner, adding an element of aesthetic appeal without overwhelming the user. The use of a QR code as a login option enhances the user's experience and provides a convenient and secure method for accessing the MinID platform. While the SMS login buttons remain available, they are downsized to encourage QR code usage, aligning with the goal of reducing costs and enhancing user security.

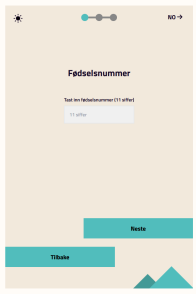

Figure 6. Implementation III

C. Implementation III

This design has the same flow as implementation I, but with a different color scheme and layout.

The design of Implementation III focuses on simplicity and ease of understanding. It employs a blocky button layout and adopts a beige and turquoise color scheme. The login process is intuitive, ensuring a hassle-free experience for users. The color scheme and layout are carefully chosen to enhance user experience and clarity, making it an appealing choice for users who prioritize simplicity when accessing public services.

VII. Discussion

In this section the results will be analyzed and compared to the initial objectives. It explores the strengths and weaknesses of the MINID-Mockups solution and discusses potential areas for improvement.

A. Implementation I

As previously stated in the implementation section, implementation 1 features a clean and user-friendly design. One of its key strengths lies in its ability to categorize users into existing, new users who have ordered an activation letter, or new users. This classification streamlines the user experience, enabling users to navigate to the appropriate website with ease. The main problem is that the implementation is providing feedback on whether a given birth number was not registered or simply redirecting the user to the login if the birth number was correct. This could be exploited for the purpose of birth number enumeration, where hackers could repeatedly input different birth numbers until they find one that exists. Until they find an existing birth number, they would receive an error message saying "this birth number does not exist," while if they find a valid birth number, they would be directed to the login page. A potential solution to the security concern could involve implementing a "Completely Automated Public Turing test to tell Computers and Humans Apart" (CAPTCHA). However, it's important to consider that introducing CAPTCHA might add another step to the user flow, which could lead to a slight increase in login time and potentially inconvenience some users. Additionally, there may be users who have difficulty completing CAPTCHA due to various reasons, such as visual impairments or other accessibility issues. Therefore, while CAPTCHA can enhance

security, it should be carefully evaluated to ensure it does not negatively impact user experience and accessibility for all users.

B. Implementation II

Implementation II presents several advantages that contribute to an enhanced user experience and improved security for the MinID platform. One of the primary benefits is the streamlined user experience achieved through the use of QR codes for login. Users who have the MinID app installed on their smartphones can simply scan the QR code, eliminating the need to manually enter personal-ID number.

In addition to the improved user experience and security, Implementation II also offers cost savings for the government. By promoting the use of QR codes, the implementation reduces the expenses associated with distributing one-time codes through SMS.

One of the weaknesses of this solution is that it may complicate the login process for users who are accustomed to using the one-time code (OTC) method. They will need to take an extra step to log in, potentially leading to confusion or dissatisfaction. Considering that a significant portion of the user base relies on the OTC method, this change could create resistance or disagreement among users.

On the other hand, promoting QR-code login could encourage the user base to transition from the OTC method, resulting in reduced costs associated with the one-time code distribution.

Another weakness is that it's not applicable to users without access to a smartphone or QR code scanning capabilities. It might also require additional education to increase adoption rates, which can be costly, but in the long term it might be worth it in order to reduce the OTC.

C. Implementation III

Implementation 3 shares a similar flow to Implementation 1, with the main difference lying in its design aspects. The design of Implementation 3 is optimized for improved user understanding and clarity. The layout and color scheme are carefully chosen to enhance user experience and make the login process even more intuitive. By leveraging a user-friendly design, Implementation 3 aims to further streamline the user flow and create a hassle-free login experience. This approach makes it particularly appealing for users who prioritize simplicity and ease of use when accessing public services. Because of security concerns implementation 2 is a better solution than implementation 1 and 3.

VIII. Conclusion

The conclusion summarizes the findings of the MINID-Mockups project and provides an overview of the achieved goals. It discusses the project's contributions to enhancing user authentication and access control for the MINID platform and highlights future possibilities for further development. The MINID-Mockups project aimed to improve the design and user flow for the MinID login process. Three prototypes were developed, each featuring innovative designs and improved user flows. Here are the key findings and implications of each implementation: Implementation 1 presented a clean and user-friendly design that categorized users into different groups for a streamlined experience. However, it faced a security challenge where hackers could exploit the feedback mechanism to find valid birth numbers. A potential solution involves implementing CAPTCHA, but it may add an extra step and impact user experience, especially for users with accessibility issues. Implementation 2 introduced QR-code login, striking a balance between security and user-friendliness. Although it reduced costs and enhanced user security, it might create complications for users accustomed to the one-time code (OTC) method. Additionally, it might not be applicable to users without access to smartphones or QR code scanning capabilities. Implementation 3 shared a similar flow to Implementation 1 but focused on an optimized design for enhanced user understanding and clarity. However, the user-friendliness might come at the expense of security. As there was limited user testing and data to confirm whether the solutions meet user needs, further research and user feedback are essential to ensure the MinID platform caters effectively to user preferences and requirements. More comprehensive user research can provide valuable insights to refine the implementations and create a well-rounded solution that meets both security and usability standards.

A. Future work

Future work should involve conducting extensive user testing and evaluation of all three implementations to identify the best combination of design elements that optimize security and user experience. By addressing the identified weaknesses and building on the strengths of each prototype, a more robust and user-friendly MinID platform can be achieved.