Sejf - funkcjonalność

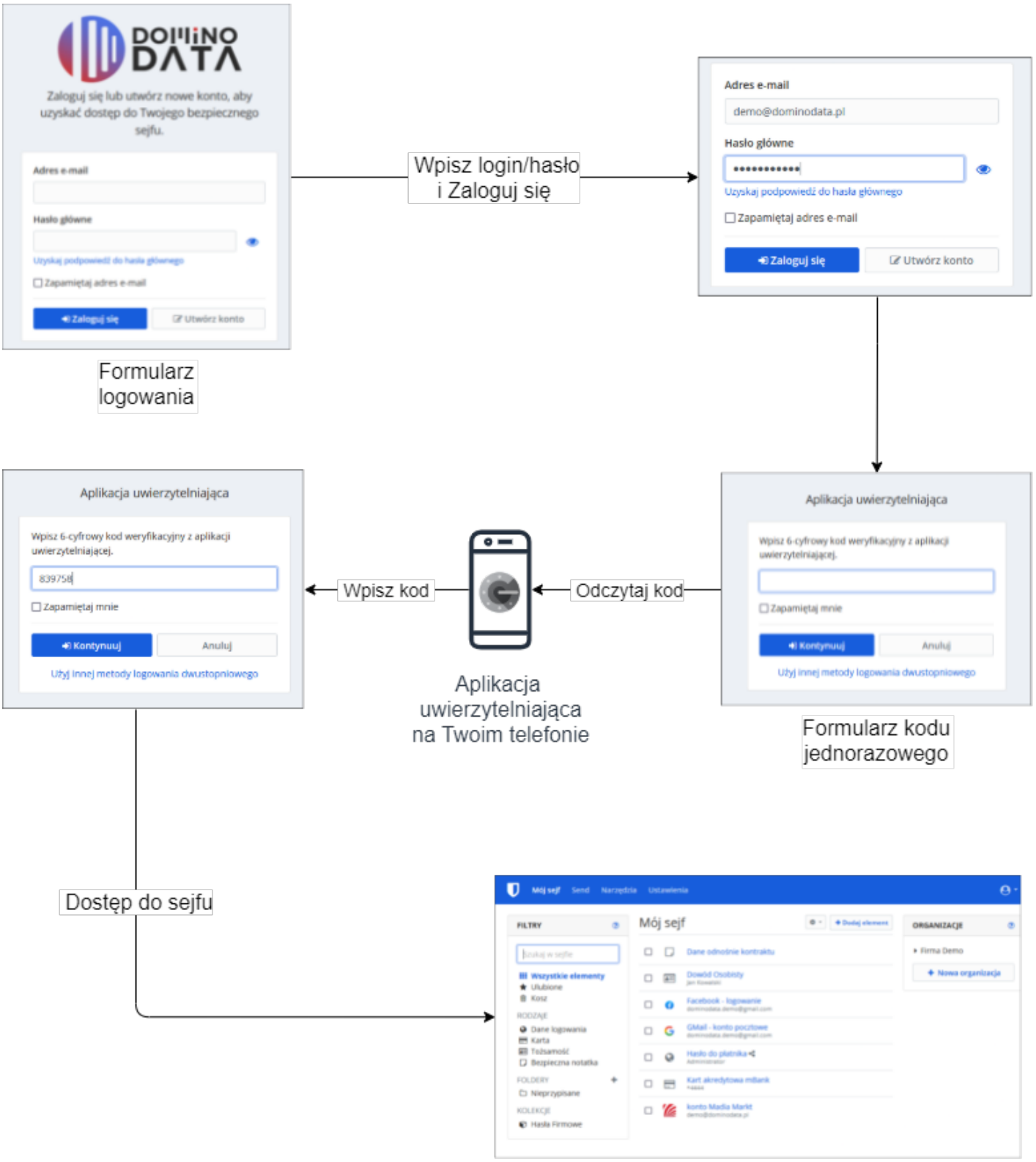
Sprawdź jak najlepiej wykorzystać możliwości sejfu

- Logowanie dwustopniowe - zabezpiecz swój sejf
- Bezpieczne wysyłanie haseł

Logowanie dwustopniowe - zabezpiecz swój sejf

Logowanie dwustopniowe BARDZO poprawia bezpieczeństwo, wprowadzając dodatkowy krok podczas logowania - wpisanie kodu z aplikacji uwierzytelniającej (instalowanej na telefonie komórkowym). Kod jest losowy i generowany co 30 sekund. Jeśli ktoś niepowołany wykradnie Twój login i hasło do sejfu, to nie będzie mógł się zalogować, gdyż nie będzie znał kodu jednorazowergo, genrowanego na Twoim telefonie.

Poniżej prosty schemat pokazujący zasadę działania logowania dwustopniowego:



Znaim skonfigurujesz logowanie dwustopniowe, musisz zainstalować na swoim telefonie aplikację uwierzytelniającą, która będzie generować kody jednorazowe. Możesz zainstalwoać jedną z poniższych aplikacji:

- Google Authenticator (iPhone, Android)
- Authy (iPhone, Android)

Poniżej możesz sprwadzić różnicę między lgowaniem zwykłym a dwustopniowym oraz zobaczyć jak aktywować logowanie dwustopniowe.

Logowanie "zwykłe" (bez kodów jednorazowych)

Włączenie logowania dwustopniowego

Włączenie logowania dwustopniowego wymaga:

- zainstalowania aplikacji uwierzytelniającej na telefonie
- podania hasła głównego do sejfu
- dodanie sejfu do aplikacji uwierzytelniającej. Gdy podczas włączania logowania dwuetapowego pojawi się poniższe okno, uruchom aplikację na woim telefonie, kliknij + aby dodać nowy wpis i zeskanuj kod QR z ekranu komputera. Po dodaniu, wpisz kod jednorazowy i kliknij włącz

- po weryfikacji, logowanie dwuetapowe zostanie włączone

Ponizszy film pokazuje proces aktywacji logowania dwustopniowego

Logowanie dwustopniowe

Bezpieczne wysyłanie haseł

Używając sejf.dominodata.pl możesz wysłać poufne informacje takie jak hasła, loginy, informacje handlowe i inne. Zamiast przesyłać je bezpośredniu w mailu, czacie itp, przesyłasz link do wiadomości. Odbiorca klika w link i sprawdza wiadomość. UDostępniona wiadomość nie "opuszcza" nigdy sejfu. Mozesz ustawić dodatkowe zabezpieczenia dla tego linku, takie jak:

- **Data usunięcia** - wiadomość zostanie trwale usunięta z sejfu w określonym czasie
- **Data wygaśnięcia** - jeśli funkcja jest włączona, dostęp do wiadomości (linku) wygaśnie po określonym czasie.
- **Maksymalna liczba dostępów** - Jeśli funkcja jest włączona, po osiągnięciu maksymalnej liczby dostępów, użytkownicy nie będą mieli dostępu do tej wiadomości (linku)
- **Hasło** - możesz opcjonalnie ustawić hasło dostępu - odbiorca będzie musiał je wpisać aby przeczytać wiadomość

Dzięki tej metodzie, w historii Twojej poczty, czatu itp. nie zostają poufne dane a jedynie linki do nich, które tracą ważnośc po jakimś czasie.

Poniżej przykłady jak tworzyć i wysyłaćpoufne dane

Utworzenie wysyłki z datą wygaśnięcia, datą usunięcia, maksymalną liczbą dostępów

Utworzenie wysyłki z datą wygaśnięcia, datą usunięcia, maksymalną liczbą dostępów, hasłem

Odczytywanie wysyłki

Odczytywanie wysyłki z hasłem