

Nonce upon a time

PRAWDA W SIECI

07.12.2025

ZESPÓŁ

APPLICATION FAIL
SUCCESSFULLY

W SKŁADZIE

FILIP OLIWA

JAROSŁAW
OPARKA

DOMINIK
DOMŻALSKI

DAWID ADAMSKI

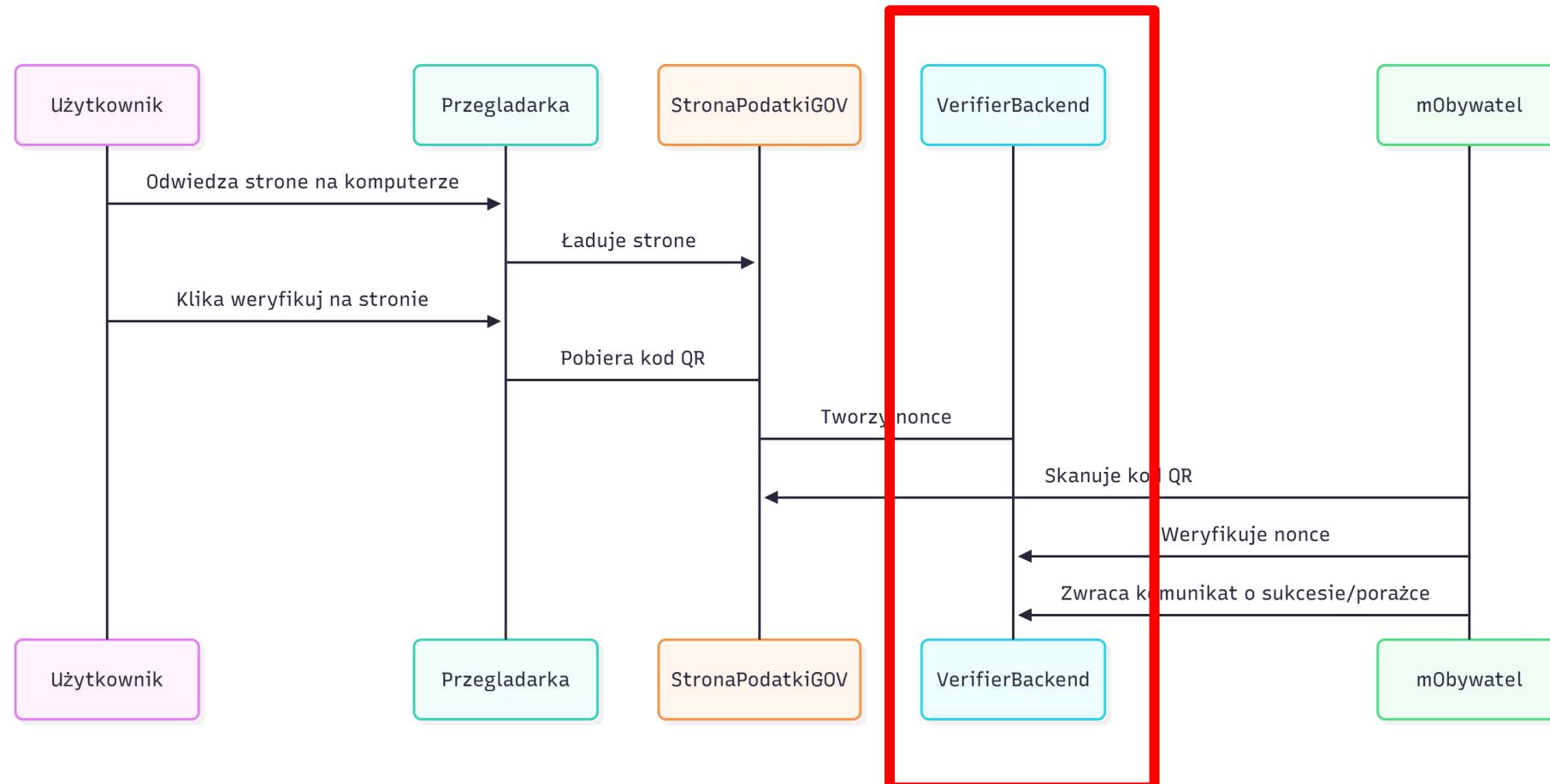
PAWEŁ LASOCKI

MIKOŁAJ PRUS

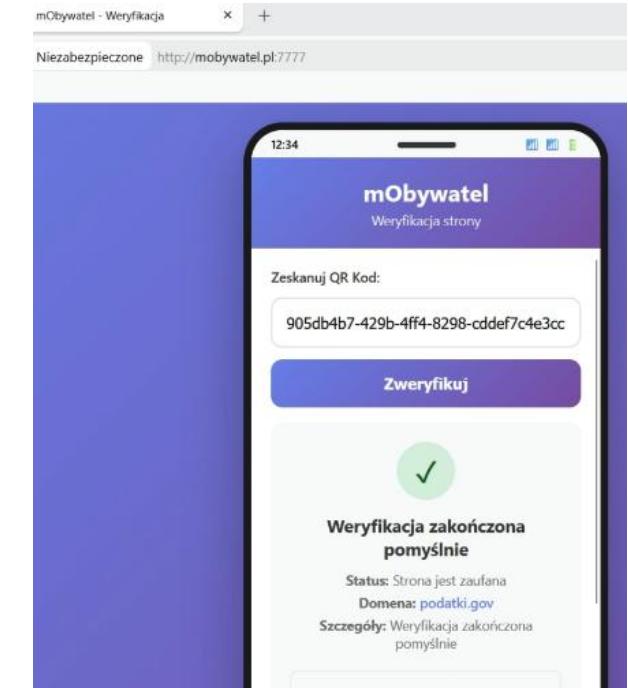
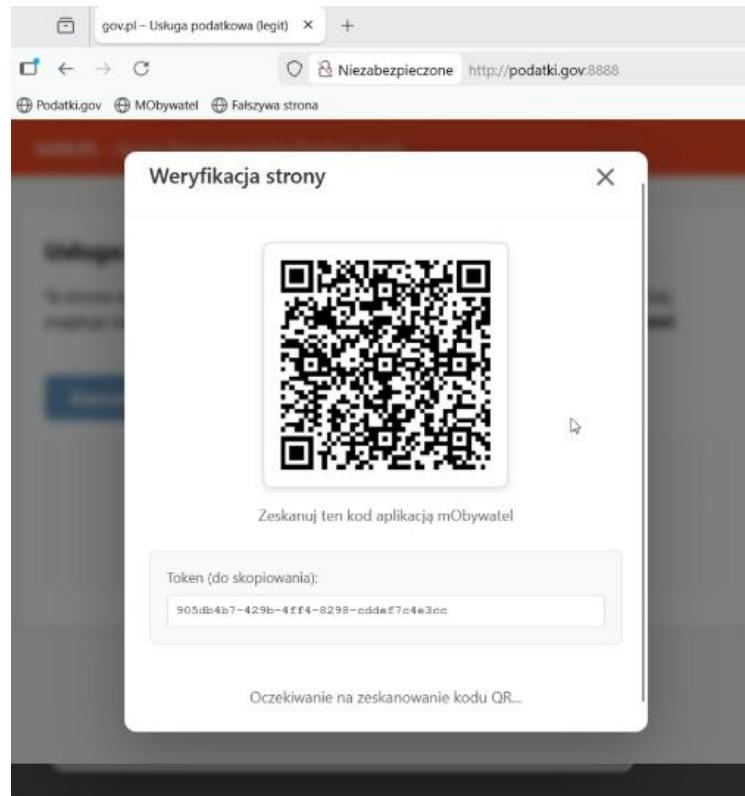
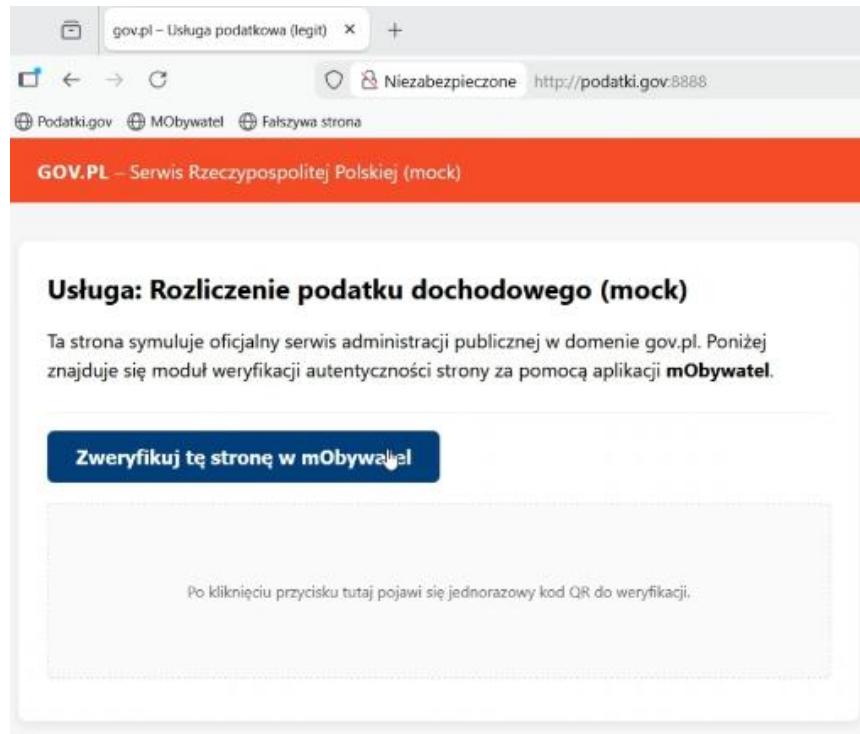
mObywatel

- ▶ Projekt pozwala na:
 - ▶ Odróżnienie stron phishingowych od prawdziwych domen administracji rządowej
 - ▶ Prosta zasada działania i implementacja
 - ▶ Weryfikacja certyfikatu SSL strony generującej kod QR
 - ▶ Przycisk na stronie wyzwala mechanizm weryfikacji (tylko na żądanie, nie przy każdym wejściu na stronę)
 - ▶ Informacja o certyfikacie SSL jest podana

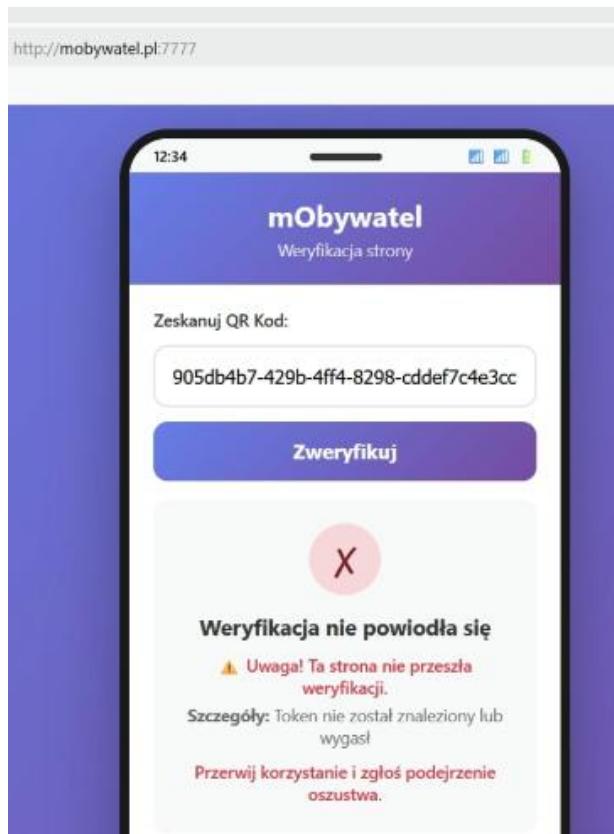
Diagram sekwencji



Scenariusz – Zaufana strona rządowa (Weryfikacja)

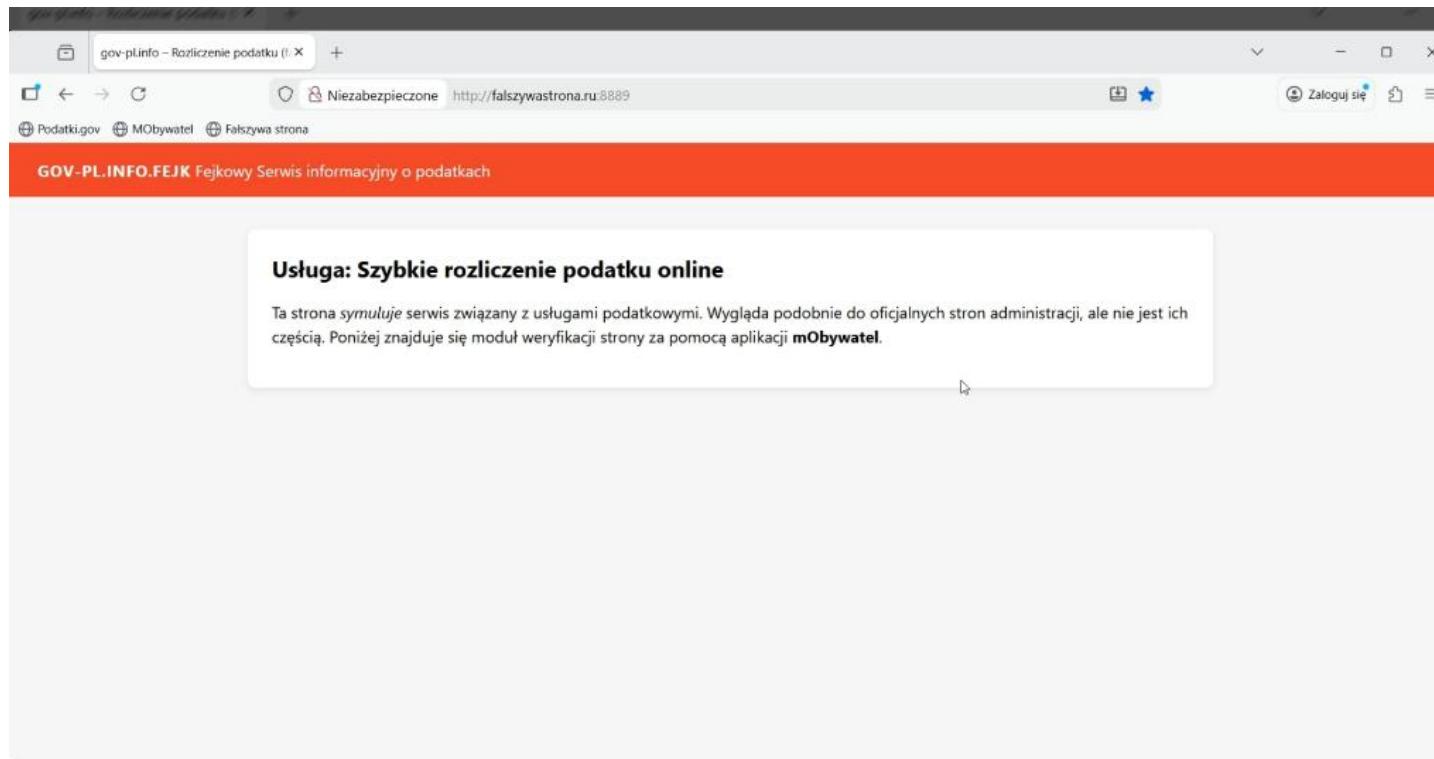


Scenariusz – Czas ważności QR kodu (60 sekund)



Scenariusz w którym tekst (nonce)
zawarty w kodzie QR wygasł

Scenariusz – Fałszywa strona (brak kodu QR)



Scenariusz – Fałszywa strona (kod QR stworzony przez atakujących)

