Ako testovať digitálne overenie identity (selfie + doklad)

Príklad  
Klient si chce otvoriť účet cez mobilnú aplikáciu. Aplikácia požiada o nahratie fotografie dokladu (občiansky preukaz/pas) a selfie na overenie zhody tváre. Po úspešnom overení systém aktivuje účet; pri chybe sa žiadosť zamietne a používateľ dostane vysvetľujúcu správu. Cieľ testovania: overiť, že proces je spoľahlivý, bezpečný, používateľsky zrozumiteľný a súladný s právnymi a ochrannými požiadavkami (GDPR/KYC).

# Ako otestovať

1. **Základné funkčné scenáre**

* Overenie procesu „end-to-end“: od otvorenia obrazovky pre nahratie dokladu až po výsledok (schválené/zamietnuté).
* Povinné polia a validácia: kontrola formátov dátumu, čísla dokladu, krajiny vydania.
* Rôzne typy dokladov: občiansky preukaz, pas, vodičský preukaz - potvrdiť akceptované typy a ich polia.

1. **UX / správy pre používateľa**

* Zrozumiteľné chybové hlásenia: čo opraviť (rozmazané foto, nekonzistentné údaje, chýbajúci roh dokladu).
* Pokyny pri snímaní: rámovanie, osvetlenie, odstránenie reflexov - testovať, či pokyny zodpovedajú realite.
* Prístupnosť: testovať s väčšími fontami, hlasovým ovládaním a na rôznych veľkostiach obrazovky.

1. **Kvalita nahraných snímok a predspracovanie**

* Rozmazanie/nízke rozlíšenie: nahratie zámerne rozmazaných alebo nízko-res obrázkov.
* Osvetlenie/tiene / odlesky: testovať na podexponovaných a preexponovaných snímkach.
* Orientácia a orez: obrázok otočený o 90/180°, časti dokladu mimo rámu.

1. **Liveness a anti-spoofing (ochrana pred podvrhmi)**

* Statické obrázky vs živé selfie: pokusy s fotografiou z iného zariadenia alebo obrazovky.
* Video vs foto liveness: ak systém podporuje video, overiť, že rozpozná pohyb, blink a 3D znaky.
* Použitie masky/tlačeného obrázka: pokusy s reálnymi scenármi útoku (papier, obrazovka, maska).

1. **Biometrické porovnanie a presnosť modelu**

* Zhoda tvár–doklad: testovať s rovnakou osobou a s podobnou tvárou (súrodenci, dvojníci).
* Nastavenie prahu zhody: zmapovať false-positive a false-negative scenáre.
* A/B test hraníc: zmerať dopad prísnejšieho/voľnejšieho prahu na UX a bezpečnosť.

1. **Bezpečnosť dát a ochrana súkromia**

* Prenos a ukladanie: overiť šifrovanie v transporte (TLS) a v úložisku (at-rest).
* Minimálny retention: či systém neukladá zbytočne dlhé kópie dokladov/selfie.
* Práva používateľa: žiadosť o vymazanie, export údajov — otestovať workflow (GDPR).

1. **Integrácia so službami tretích strán (KYC/AML)**

* Chybové stavy od poskytovateľa: simulovať downtime, timeout, nevalidné odpovede.
* Mapovanie kódov odpovedí: že klient vidí zmysluplnú správu (napr. „overenie zlyhalo“ vs „chyba služieb“).
* Retry a idempotencia: opakované pokusy nemajú vytvoriť duplicitné záznamy.

1. **Load, škálovateľnosť a rate limiting**

* Paralelné nahrávania: otestovať správanie pri veľkom počte súbežných overení.
* Rate limits od providera: overiť správne zobrazenie chybových hlásení a spätnú logiku (exponenciálne znovupokusy alebo fallback).

1. **Logging, audit a sledovateľnosť**

* Audit trail: zaznamenané kroky (časy, výsledky, chybové kódy) bez úniku citlivých údajov.
* Monitorovanie anomálií: nastaviť alerty pri zvýšenom počte odmietnutí alebo podozrivých aktivít.
* Reprodukcia incidentu: uložiť metadáta potrebné na debugging (bez ukladania priamo citlivých obrázkov, ak to nie je povolené).

1. **Negatívne scenáre a hraničné prípady**

* Nesprávne metadáta (falošný dátum narodenia), či systém nájde nekonzistentnosti.
* Zmeny dokladu (opotrebenie, malé poškodenie): overiť toleranciu systému.
* Migrácia medzi zariadeniami: nahratie selfie z iného zariadenia/účet prihlásený na inej IP.

**#testing #qa #digitalidentity #biometrics #KYC #privacy #security #banking #ux #gdpr**