Az “uklogin” Openid szolgáltatás adatkezelési folyamatai

ügyfélkapus hitelesítést használva
(később a tervek szerint lesz más fajta hitelesítési lehetőség is, ezekről maj másik ilyen leírás készül)

1. Felhasználó regisztrálás folyamata

a. A felhasználó bejelentkezik a magyarorszag.hu rendszerbe (ehhez un “ügyfélkapu hozzáférés” szükséges, amit az okmány irodákban lehet kérni)
https://magyarorszag.hu
Ez az adatkezelés a magyarorszag.hu szerveren történik. Adatkezelési leírása: https://www.nyilvantarto.hu/ugyseged/Tajekoztato.xhtml

b. Innen letölti az ott tárolt személyes adatait pdf fájl formájában
https://www.nyilvantarto.hu/ugyseged/NyilvantartottSzemelyesAdatokLekerdezeseMegjelenitoPage.xhtml
Ez az adatkezelés is a magyarorszag.hu szerveren történik. Adatkezelési leírása: https://www.nyilvantarto.hu/ugyseged/Tajekoztato.xhtml
A letöltött pdf adattartalma:
- jelenleg viselt teljes név
-személyi azonosító (személyi szám)
-születési dátum
-neme
-előző családi név
-születési név
-anyja neve
-állampolgársága
-születési hely
-családi állapot
-nyilvántartás jogcíme
-adatait letiltotta (igen vagy nem)
-állandó lakcím (postai irányító szám település utca házszám stb)
-bejelentés dátuma
-kijelentés dátuma
-fiktívvé nyilvánítás dátuma
-cím státusza
-tartózkodási hely (ha eltér a lakcímtől)
-személyazonosító igazolvány adatok (okmányazonosító, arckép van vagy nincs, érvényességi idő, érvényesség ténye, aláírás igen vagy nem)
-személyi azonosítót és lakcímet igazoló hatósági igazolvány adatok (okmány azonosító, érvényesség ténye)

c. A user a letöltött pdf fájlt elektronikusan aláírja a kormányzat által ingyenesen biztosított elektronikus aláírási szolgáltatás segítségével

https://szuf.magyarorszag.hu/szuf_avdh_feltoltes
Ezt az adatfeldolgozát is az ugyfelkapu.hu rendszer végzi. Adatkezelési tájékoztató:
https://magyarorszag.hu/snap/repo/one_page.php?page_id=7272088405119076&panel=L#

Az aláírási folyamat során a pdf adattartalma kiegészül a következőkkel:
- aláírás szolgáltató adatai
- aláírás időpontja
- az aláírást kezdeményező személy születési neve, jelenlegi viselt neve, anyja neve, születési dátuma.

d. A user az aláírt pdf fájlt feltölti az “uklogin” Openid szerverre.

Itt az “uklogin” szerver a következő adatfeldolgozást végzi:
- az aláírásban szereplő születési név, születési dátum és anyja neve adatból képez egy “sha256 hash” kódot (továbbiakban “**idhash**”),
- kiemeli a pdf-ből a következő “**kezelt user adatok**” -at: jelenlegi viselt név, állandó lakcím, tartózkodási hely, születési dátum, anyja neve, neme.
- a pdf -ben szereplő többi adatot nem kezeli, a feltöltött pdf -et a feldolgozás után (1-2 másodperc) azonnal törli.
- ezután a user a képernyőn további kiegészítő adatokat ad meg magáról: (nickname, password, email cím, avatar kép url, személyes web oldal url)
- elfogadja a képernyőn megjelenő link segítségével olvasható “uklogin rendszer adatkezelési tájékoztatója” -t.
- ha mindez megtörtént akkor létrejön egy új user rekord. A rekordban az “**idhash**”, a “**kezelt user adato**k”, a nickname, email, avatar url, személyes web url és a user jelszó hash256 kódja szerepel, valamint a létrehozás dátuma.

2. Használat

Amikor egy kliens program user bejelentkezést kezdeményez akkor elküldi az “uklogin” Openid szervernek a
- kliensId -t (a regisztrált kliens prg azonosítója)
- azt, hogy milyen user adatokat kér (pl. nicknév, teljes név, lakcím, email)
- kiegészítő infok (ezeket az “uklogin” nem kezeli, hanem változtatás nélkül visszaküldi majd a kliensnek, technikai okokból lehet erre szükség)

az “uklogin” szerver megjeleniti a login képernyőt, a képernyőn szerepel:
- bejelentkezési név input box
- jelszó input box
- kliens app megnevezése
- a kliens app EU-n belüli vagy nem
- az “uklogin” Openid szerver adatkezelési leírására mutató link

- a kliens prg adatkezelési leírására mutató link
- a kliens prg által kért adatok köre (pl. teljes név, email, lakcím)
- checkbox, hogy a user hozzájárul mindkét adatkezeléshez

Az képernyő elküldése után, sikeres user azonosítás után a kliens app vissza kapja a vezérlést, és le tudja kérni a meghatározott user adatokat.

3. Naplózás

Az “uklogin” szerver naplót vezet arról, hogy melyik user, mikor, melyik applikációnak milyen adatok átadásához járult hozzá. Ez a napló titkosítottan van tárolva egy olyan adatbázisban amihez írási joga csak a wb programnak van, olvasási joga csak a rendszergazdának. A titkosított adatokat dekodolni csak a felelős adatkezelő személy tudja (a nála USB tárolón lévő privát kulcs segítségével) Ez azt jelenti, hogy a napló adatok tartalmához csak a rendszergazda és a felelős adatkezelő együtt tud hozzáférni. Az ilyen hozzáférésről kötelesek írásos jegyzőkönyvet vezetni.

A napló adatokat kizárólag a user kérésére, vagy adatkezelési vitákban a bizonyítási eljárás céljára használjuk fel, ezen kivül harmadik félnek csak akkor adjuk ki ha erre bennünket törvény kötelez.

4. Adatbázis

userek

id,
nickname,
pswhash,
“kezelt user adatok”
avatar
email
személyes web oldal url
létrehozás dátuma

napló

userid
időpont
clientid
átadott adatok (pl nickname, email)
link az adott időpontban érvényes uklogin adatkezelési leírása
link az adott időpontban érvényes kliens adatkezelési leírásra

kliensappok

clientid
megnevezés
domain
default callback url
default adat kör
adminok
pubkey
adatkezelési leírások (több verzió)

5. Adatkezelés leírások kezelése

Az “uklogin” adatkezelési leírásokat a rendszergazda viszi fel, minden módosításnál új példány keletkezik, verzió szám is tartozik hozzá. A login folyamatnál mindig az utolsóra (aktuálisra) mutató link jelenik meg, de a korábbi verziók is tárolva vannak.

A kliens adatkezelési leírásait a klienst regisztráló user tölti fel. Lehetősége lesz az adatkezelési leírást később frissíteni, ilyenkor mindig új példány keletkezik, verzió számozással, de a korábbiak is megőrződnek. A login folyamatban mindig a utolsóra mutató link jelenik meg.

6. User adatmódosítás

   Bejelentkezés után a user saját profiljában csak azokat az adatokat módosíthatja amik nem az ügyfélkapuból lettek lekérve tehát:
   - jelszót változtathat
   - email címet, avatar URL -t, személyes web URL -t változtathat.

7. User adat törlés lehetősége

   Bejelentkezés után a user a “profil” formon lévő “fiókom törlése” gombra kattintva (megerősítő popup kérdés után) törölheti a teljes rá vonatkozó user rekordot. A napló rekord nem törlődik mivel biztonsági okokból a web prg-nak nincs erre jogosítványa. Viszont így a napló rekordban olyan bejegyzések maradnak amiknek a userId -je már nem mutat valós user rekordra, tehát ezek már nem személyhez köthetőek. Mivel az adat kezelési vita vagy user kérésre történő manuális napló lekérdezések egy-egy adott userrel kapcsolatban történnek, ezek a nem személyhez kötött rekordok nem okoznak problémát. Ha valamiért mégis teljes körű adatlekérés válna szükségessé, akkor megfelelő sql kóddal kezelhető ez a helyzet is.

8. User adatlekérési lehetőségei

   Bejelentkezés után a user a “profil” formon lévő “adataim lekérése” gombra kattintva kérheti a user rekord tartalmát json formátumban. A napló olvasására web programnak nincs lehetősége, a napló adatainak lekérését emailben kérheti a felelős adatkezelőtől, ez esetben az adatkezelő és a rendszergazda együttműködésével manuális munkával (sql query) előállítják a kért napló részletet CSV formátumban, jegyzőkönyvet vesznek fel erről az akcióról, és a csv fájlt elküldik a usernek.

9. Kliens applikáció regisztrálása

   Az uklogin -ba beregiszrált (hiteles fiókkal rendelkező) userek tudnak bejelentkezés után új kliens app-t regisztrálni. Annak bizonyítására, hogy ők az adott kliens app rendszergazdái egy meghatározott tartalmú fájlt kell az app root könyvtárába feltölteniük. Az app megadandó adatai:
   - megnevezés
   - domain
   - default callback url
   - default adatkérési kör (pl. nickname, lakcím)
   - adatkezelési leírás (pdf feltöltés)
   - checkbox nyilatkozat arról hogy az app megfelel a GDPR előírásoknak
   - az app adatkezelés EU-n belül történik (Igen vagy nem)
   - amennyiben fokozott titkosított user adatátadást kér, akkor publiikus kulcs
   - kliens adminisztrátorok (nicknév lista)

Megjegyzés: Mivel a rendszer csak https: kommunikációt támogat, a kliens és az uklogin szerver közötti adatforgalom eleve titkosított. A megadható pubkey -s titkosítás ezen felüli fokozott biztonságot adhat; ez esetben a user adat “JWE” szabvány szerinti kódolt tokenkenben kerülnek átadásra, ha ezt nem kérte akkor JSON stringként (de ilyenkor is a https miatt titkosítva).

10. Kliens applikáció regisztrálás módosítása

A kliens regisztrációban felsorolt kliens adminisztrátorok bejelentkezés után módosíthatnak minden kliens app adaton. Ha új adatkezelési leírást töltenek fel, akkor a régi is megőrzésre kerül, új verzió szám képződik. A kliens adminisztrátorok közül önmagát nem törölheti az éppen bejelentkezett user.

11. Kliens applikáció regisztrálás törlése

A kliens adminisztrátorok bejelentkezés után (biztonsági popup megerősítés után) törölni tudják a kliens app rekordot az adatbázisból.

Kérdés: a kliens rekordokkal kapcsolatos adatmanipulációkat naplozzunk vagy ne?

Gondolom kellne még valami szabályzat a napló lekérdezésekről vezetett jegyzőkönyvek kezeléséről, az adatbázis archiválások, visszaállítások kezeléséről, a napló megörzési idöről, a rendszergazdai adatjogosultságokról……

GDPR dokumentáció struktúra:

Ezeket kell végiggondolni, ez alapján össze lehet rakni a szükséges dokumentumokat:

Publikus:

Adatkezelési leírás,
Nyilatkozat
Kapcsolat (hol tud adatigénylést leadni)

Belső:

Adatkezelési szabályzat,

Adatkezelési nyilvántartás

Adatkezelés célja	**Adat forrása**	**Kezelt adatok**	**Adatkezelés**	**Jogalap**	**Megőrzési idő**	**Érintett rendszer(ek)**	**Továbbítás**	**Adatkezelési leírás**	**Nyilatkozat szükséges**
Felhasználó regisztrálás	Felhasználó	Keresztnév Vezetéknév	Új regisztráció létrehozása (részletesebb leírás)	Jogos érdek	3 hónap	openID szerver, adatbázis (ha van külön)	Nem	Link, vagy szabályzat neve	Igen
pl.: Felhazsnáló adatlekérés	pl.: Ügyfélkapu	pl.: Keresztnév Vezetéknév	Új regisztráció adatlekérdezés	Jogos érdek	3 hónap	openID szerver, adatbázis (ha van külön)	Ügyfélkapu	Link, vagy szabályzat neve	Igen

11:20

A táblázatot azért szeretem mert tételesen végig lehet követni honnan, mi, miért, hová megy