

Užívateľská príručka

Tento dokument vznikol ako užívateľská príručka pre webové aplikácie vydavateľa a overovateľa. Obom je venovaná samostatná podkapitola, v ktorej je predstavený spôsob inštalácie potrebných závislostí umožňujúce spustenie. Pre každú aplikáciu budú popísané funkcie a jedinečné vlastnosti, ktoré poskytujú. *Inštalácia a spustenie aplikácií bolo vykonané na linuxovej distribúcii **Ubuntu 20.04**.*

Webová aplikácia vydavateľa

Aplikácia je postavená na kontajneroch Docker, ktoré sú spravované nástrojom **docker-compose**. Obe spomenuté technológie nie sú súčasťou OS a preto je potrebné vykonať inštaláciu. Postup inštalácie sa nachádza na oficiálnej stránke [Dockeru](#) a [Dockeru Compose](#).

Spustenie aplikácie

Zdrojový kód webovej aplikácie sa nachádza v repozitári **GitLabu**. K získaniu repozitáru je potrebné mať nainštalovaný nástroj **git**.

```
$ sudo apt-get install git
$ git clone git@gitlab.com:brno-axe/mvcr-adiopsio/web-adopsio.git
```

Po úspešnom naklonovaní je potrebné nasmerovať sa do pracovného adresáru kde sa nachádza konfiguračný súbor **docker-compose.yml**. Následne je potrebné vytvoriť 3 konfiguračné súbory, v ktorých sa nastavujú parametre aplikácie. Konkrétne sa jedná o súbory s názvami

- **.env.prod** - obsahuje konfiguráciu Flasku

```
FLASK_APP=wsgi.py
FLASK_ENV=production
SECRET_KEY=<secret>
DEBUG=False
TESTING=False
SQL_HOST=db
SQL_PORT=5432
DATABASE=postgres
DATABASE_URL=postgresql://<username>:<passwd>@db/<databaze>
# Google API
GOOGLE_CLIENT_ID=<google_client>
GOOGLE_CLIENT_SECRET=<google_secret>
GOOGLE_DISCOVERY_URL=<google_url>
```

Nastavenia GOOGLE je možné získať registráciou aplikácie do [cloudu Google](#).

- `.env.pgadmin.db` - obsahuje nastavenie pgAdminu4

```
PGADMIN_DEFAULT_EMAIL=<email_pgadmin>  
PGADMIN_DEFAULT_PASSWORD=<passwd_pgadmin>
```

- `.env.prod.db` - obsahuje nastavenia databáze PostgreSQL

```
POSTGRES_USER=<user_db>  
POSTGRES_PASSWORD=<passwd_db>  
POSTGRES_DB=<db_name>
```

Pri prvotnom spustení je potrebné inicializovať databázu. To je možné za pomoci skriptu vytvoreného Flaskom.

```
$ docker-compose run flask-backend python3 manage.py create_db
```

Po zadaní príkazu sú vytvorené všetky tabuľky a vstreknuté seed dáta - preddefinované role užívateľov. Po úspešnom nastavení všetkých parametrov stačí spustiť aplikáciu pomocou nástroja `docker-compose`.

```
$ docker-compose up -d --build
```

Přepínač `-d` potlačí logovacie vypisy na pozadie a přepínač `build` umožňuje postavenie všetkých komponent.

Nastavenie webového prehliadača

Pre ukážku je použitý webový prehliadač **Firefox**, ktorý umožňuje nastavenie **http proxy**. Tento krok je potrebný kvôli možnosti presmerovania komunikácie na nastavené doménové meno serveru.

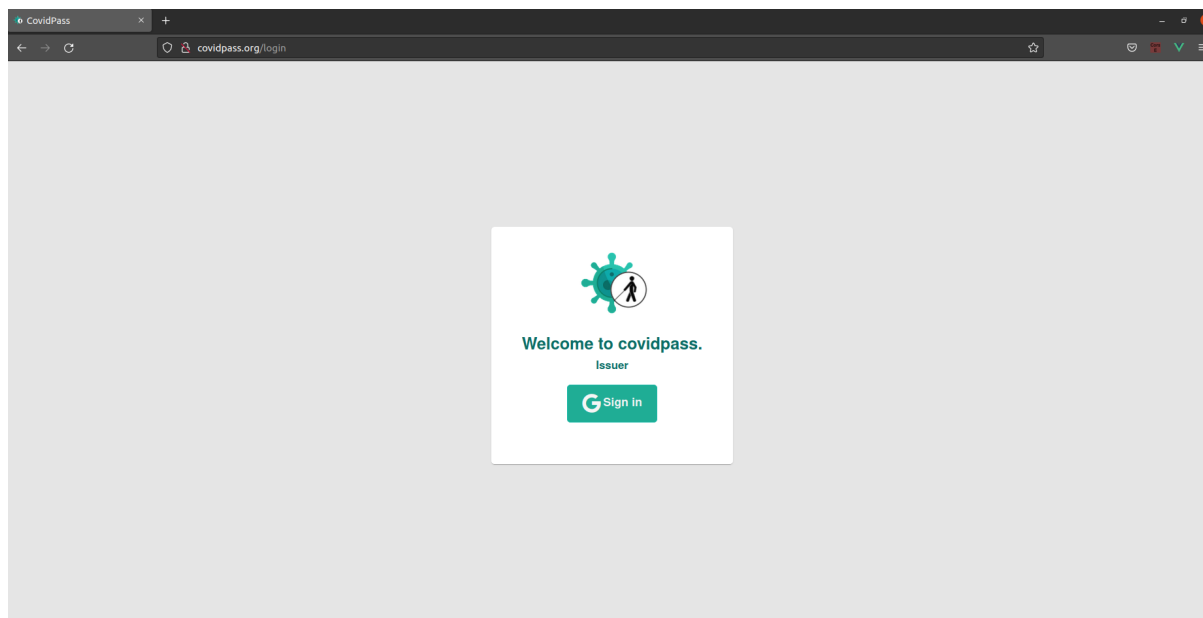
POZNÁMKA: Tento spôsob je použitý z dôvodu nasadenia aplikácie na VM server, ktorý je prístupný z VPN (pri použití privátnej adresy serveru nebude fungovať presmerovanie užívateľov k Google Auth).

Nastavenie http proxy sa nachádza v nastavení prehliadača v sekcii **nastavenia siete**. Po zobrazení dialógového okna je potrebné zvoliť ručné nastavenie a pridať buď adresu serveru, alebo **localhost**. Obe používajú port **8000**. Na uvedenom obrázku sa nachádza nastavenie http proxy použitím privátnej adresy serveru.



Zobrazenie webovej aplikácie

Po úspešnom nastavení aplikácie zadáme covidpass.org do webového prehliadača. Tento názov prezentuje webovú aplikáciu vydavateľa. Ako prvé sa užívateľovi zobrazí prihlasovacia stránka, obsahujúca logo a tlačidlo **Sign up**.





Po kliknutí tlačidla, bude užívateľ presmerovaný a vyzvaný k prihláseniu pomocou účtu registrovaného v Google. Ak sa užívateľ nenachádza vo webovej aplikácii vydavateľa, bude vyzvaný k registrácii, ktorá slúži k získaniu informácií o užívateľovi na základe, ktorých mu budú vytvorené digitálne certifikáty. Na ľavom obrázku sa nachádza prihlásenie pomocou Google a na pravej registrácia v aplikácii vydavateľa.


Přihlásit se přes Google

Vyberte účet

a pokračujte do aplikace covidpass.org

 **UserName UserSurname**
covidpass.user@gmail.com

 **Roman Klampár**
fekt.covidpass@gmail.com

 Použít jiný účet

Budete-li pokračovat, Google bude sdílet vaše jméno, e-mailovou adresu, předvolbu jazyka a profilovou fotku s aplikací covidpass.org.

Firstname

Surname

Birthdate

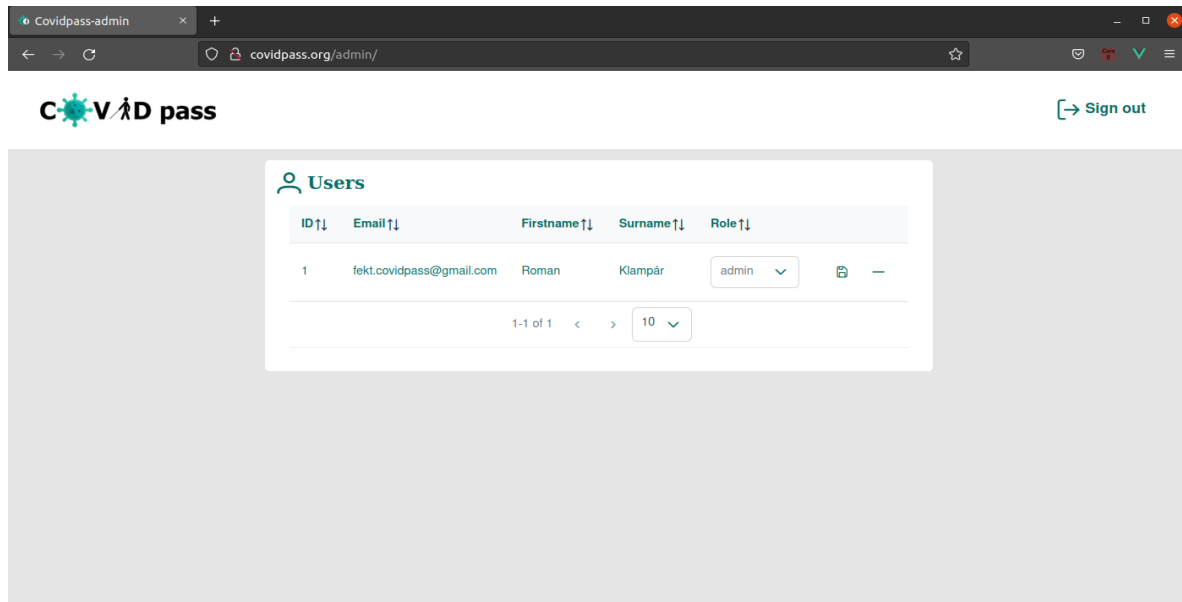
Email

Signup

Close

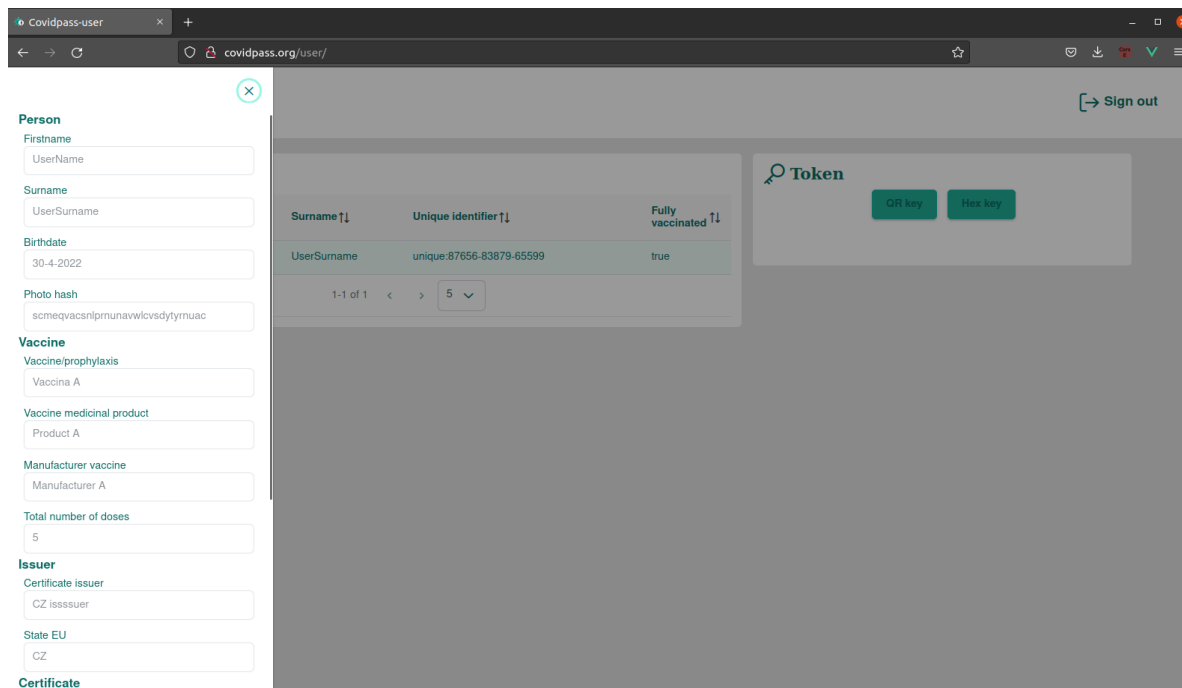
Admin

Prvý užívateľ registrovaný vo webovej aplikácii automaticky získa rolu **admin**, ktorý bude môcť spravovať všetky registrované účty užívateľov. Môže ich mazať poprípade meniť role. Po zmenení role je potrebné túto zmenu potvrdiť kliknutím na ikonu **diskety**. Po zmazaní užívateľa, sú zmazané aj jeho existujúce certifikáty.



User

Ďalší registrovaný užívateľia automaticky získajú rolu **user**. Na tejto stránke sa nachádza tabuľka obsahujúca všetky vytvorené digitálne certifikáty užívateľa. Po kliknutí na riadok certifikátu sa zobrazí sidebar, v ktorom sa nachádzajú všetky informácie obsahujúce certifikátom.



Na tejto stránke sa taktiež nachádza sekcia **Token**, ktorá sprístupňuje jednorázový API kľúč určený k získaniu digitálnym certifikátom prostredníctvom koncového bodu covidpass.org/user/certs. Token je možné zobrazíť v QR podobe, ale taktiež v hexadecimálnej.

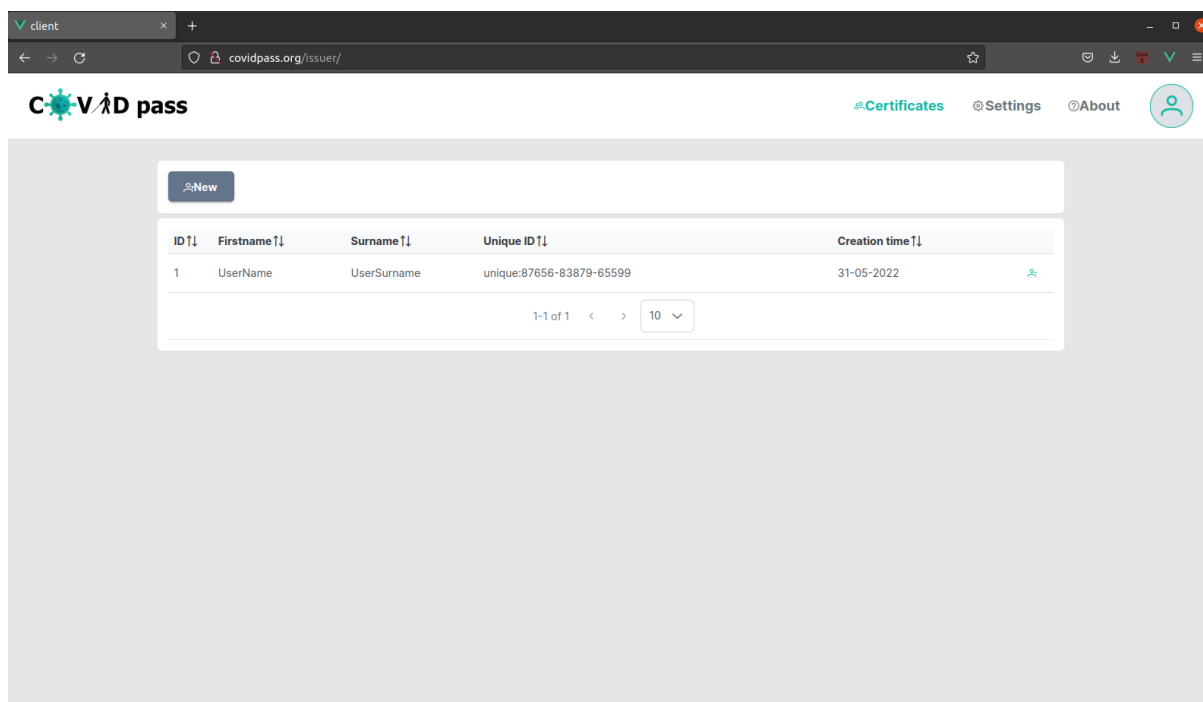
```
$ curl covidpass.org/user/cert -proxy 192.168.6.6:8000 -h 'X-API-KEY: <KEY>'
```

Po použití tohoto dotazu je vrátený digitálny certifikát vo formáte JSON, ktorý sa skladá z dvoch častí a to **certificate** - obsahuje raw data, a **sigma** - obsahujúca podpísané atribúty.

```
1 {
2   "status": true,
3   "creation_time": "01-05-2022",
4   "email": "covidpass.user@gmail.com",
5   "certificate": {
6     "firstname": "UserName",
7     "surname": "UserSurname",
8     "birthdate_day": "5",
9     "birthdate_month": "3",
10    "birthdate_year": "2022",
11    "photo_hash": "whnquipwmyxnuqccisswldarheqfzgp",
12    "unique_id": "uuid:dasbczxc-dscnjsd-542368-dasczn",
13    "vaccination_day": "10",
14    "vaccination_month": "4",
15    "vaccination_year": "2022",
16    "dose": "5",
17    "total_dose": "10",
18    "completed_vaccination": "False",
19    "vaccine": "Vaccine A",
20    "product": "Product A",
21    "manufacturer": "Manufacturer A",
22    "issuer": "CZ issuer",
23    "state_eu": "CZ",
24    "optional1": "Brno",
25    "optional2": "B007"
26  },
27  "sigma": {
28    "sigma_0": "1 1416643728770404541173183613019758649575772763209612449606972807866879893296 8726769614300335467247273800368583940810892300027561158749967369556871074336",
29    "sigma_1": "1 7013038374791945901009399974281094724593828494536702850816639180109553195113 6037421768854728589528201864023835974427947207544687736723333276565183411524",
30    "sigma_2": "1 88672148710520155827655057647298832095428786808148049777866009631160537381862 516547542381191671969356779334803850193737382772127124027707925149819946140",
31    "sigma_3": "1 128277014443278072805519293319699268119250337726942688715227697433943592680 922871310742838885430036834746474807989515867505905682454211120358534252617",
32    "sigma_4": "1 1435638110202057938898425694113490684262269659932906826496358959308633769891 8034790518327025316663159641333841910699747791930663702072140337240357599071",
33    "sigma_5": "1 4774897405188908938983402221003176700937352999590910351244870952083856022275 7069866433463808028555960841770159104342549417767458886531157422569658101386",
34    "sigma_6": "1 10957918837848303643965092702962781755964084074301906597887635699025027298316 6622307819437640633378515785988427453907400686302679557485602042312607470050",
35    "sigma_7": "1 37067832996175441966338937808050161484376619687687103725747870007133804463360 727210477995916793464722364840215303526830941039017365465742295369754882741",
36    "sigma_8": "1 4271950796957409068867202915697433129698934292232159655102085312391399692565 1601372282574412830271823496122315310918270995436698489919965631598808020633",
37    "sigma_9": "1 12282781654974265936161040946481952814192945439895933780412082213886707678874 10036148681114123487844117424262552209453582892746672843806466077098687643820",
38    "sigma_10": "1 16595783475487344021652716074710895979854213924075147966637974299336054523379 1366608168105658294900460506321874983721853936727839948420683817976489281085",
39    "sigma_11": "1 13706767742636332511993152079734029112442005235150011827832583102746464601 98431270039096758754820932761388018334406817199486622414359570907490461925",
40    "sigma_12": "1 4222790973355610731177057852949532440517135708784110106103115806625785934001 15226884780378640894451960858303632021307595529820150094476298532389400627046",
41    "sigma_13": "1 584459288404260748342303553874669266353462656845904229600779075474824508731 13002807848022202596257224451224169933422692454213961359257547144670412207344",
42    "sigma_14": "1 8020751873570533511218504186087541010237710636378158944331486243909322154 7480578937525315157621393296259011026439501230271521715781160327552562020341",
43    "sigma_15": "1 10230478085834707025592656136068795981761829000068312864763762341520529538587 9942295380165304633490339285161061893231200743790389364578171554129694184555",
44    "sigma_16": "1 12751731875206291641865558413484887189628594718630438110491227901081486836934 1530820100858456360184135143139546239710018267504722990959417223894726412275",
45    "sigma_17": "1 766247626384651113013345500872841820694237214309654260400823683020751016534 1284894689018914106759322435451091164544746512018937362104210989807058401030",
46    "sigma_18": "1 8849063548539673236714914874314032364835536911107523080361788337451354801533 1009236150628965095091409684318817931119356215639029958079295550414326728035",
47    "sigma_19": "1 15860163693679904453592937991520866445036967267492944218669134188648085161075 997424286049237987663751403341265152704329325882725693514084526022743784617",
48    "sigma_20": "1 1418919199384912578482815687049593501940839521817525459775129130140231859643 5580892776477711055790522228587583349974010167516631066308483438358407468192"
49  }
50 }
```

Vydavateľ

Poslednou je časť určená pre vytváranie nových certifikátov. Skladá sa z 3 podstránok, **certificates**, **settings** a **about**. Úvodná stránka je **certificates**, ktorá zobrazuje všetky doteraz vytvorené certifikáty, ktoré môže vytvárať ale aj mazať. Mazanie je realizované stlačením ikony, po ktorej sa zobrazí potvrdzovacie dialógové okno, ktorým sa potvrdzuje trvale vymazanie.

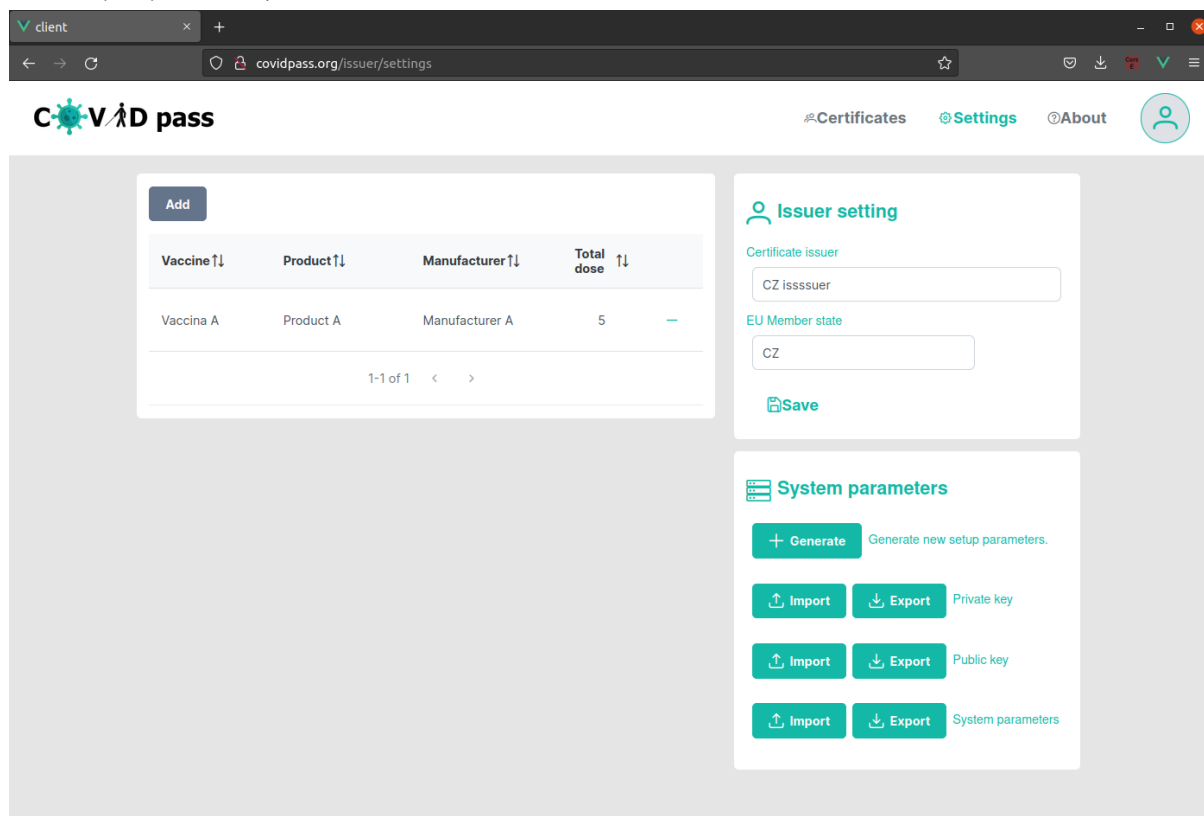


K vytvoreniu nových certifikátov slúži tlačidlo **New**, ktoré po stlačení zobrazí dialógové okno vo formáte formuláru. Sekcia **Person** sa doplní automaticky vybraním **emailu** registrovaného užívateľa. Obdobne to funguje aj pri sekcii **Vaccine**. Blok **Issuer** nie je možné zmeniť z dialógu.

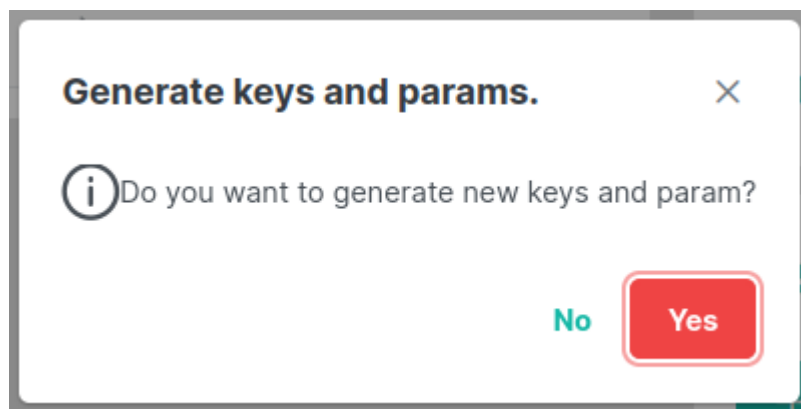
The 'New certificate' dialog form is divided into several sections. The 'Person' section contains fields for Email (covidpass.user@gmail.com), Firstname (UserName), Surname (UserSurname), and Birthdate (01-05-2022). The 'Vaccine' section contains fields for Vaccine/prophylaxis (Vaccina A), Vaccine medicinal product (Product A), Manufacturer vaccine (Manufacturer A), and Total number of doses (5). The 'Issuer' section contains fields for Certificate issuer (CZ issuer) and EU member state (CZ). The 'Optional' section contains fields for Optional 1 (Brno) and Optional 2 (B007). The 'Certificate' section contains fields for Unique certificate identifier (unique:87656-83879-65599), Dose number (5), and Date of vaccination (24-05-2022). At the bottom right, there are 'XNo' and '✓Yes' buttons.

Ďalšou stránkou je **settings**, ktorá obsahuje všetky potrebné nastavenia pri vytváraní certifikátu. V ľavej časti sa nachádza tabuľka obsahujúca všetky registrované vakcíny, ktoré je možné jednoducho doplniť

stlačením tlačidla **Add**. Následne sa zobrazí obdobne dialógové okno ako v prípade vytvárania certifikátov.



V pravom hornom rohu sa nachádza jednoduchý formulár, ktorý obsahuje informácie o vydavateľovi. Tieto informácie sú zobrazené v každom certifikáte vytvorených konkrétnym vydavateľom - dalo by sa povedať, že je to identifikátor inštitúcie. V ľavom dolnom rohu sa nachádzajú nastavenia atribútového autentizačného systému. Možnosť **generate** spôsobí generovanie nových **parametrov**, vrátane **súkromného** a **verejného** kľúča. Po stlačení sa zobrazí potvrdzovací dialóg, aby užívateľ upozornil na túto operáciu. V aktuálnej verzii funguje možnosť **exportovania** jednotlivých parametrov, ktoré sa stiahnu vo formáte JSON.



Webová aplikácia overovateľa

Ako názov napovedá hlavnou úlohou tejto webovej aplikácie je overovanie platnosti digitálnych certifikátov. V tejto časti je popísanie použitia GUI, pretože aktuálne nie je spojený so skriptom určeným na overovanie - projekt iného študenta.

Spustenie aplikácie

Aplikácia overovateľa nepoužíva kontajnere a preto je nutné manuálne nastaviť požadované nástroje. Jedným z nich je databáza PostgreSQL, ktorá sa musí nainštalovať.

```
$ sudo apt install postgresql postgresql-contrib
```

Po úspešnom nainštalovaní je nutné spustiť službu.

```
$ sudo systemctl start postgresql.service
```

Overenie stavu služby je možné pomocou príkazu.

```
$ sudo systemctl status postgresql.service
```

Webová aplikácia sa nachádza v repozitári na **GitLabe**, preto je ju potrebné naklonovať.

```
$ git clone git@gitlab.com:xhimorin/web-verifier.git
```

Po úspešnom naklonovaní je potrebné vstúpiť do pracovného adresáru a stiahnuť závislosti pre prácu s Pythonom. Konkrétne sa jedná o správcu balíkov **pip** a **virtualenv**, ktorý spravuje všetky závislosti projektu separátne od globálnych. Posledný príkaz inštaluje všetky používané závislosti zo súboru **requirements.txt** - obsahujú konkrétne verzie.

```
$ sudo apt install python3-pip
$ sudo apt install python3-virtualenv
$ virtualenv venv
$ . venv/bin/activate
(venv)$ pip3 install -r requirements.txt
```

Rovnako ako aplikácia vydavateľa tak aj overovateľ potrebuje parametre, ako napríklad prístupové údaje použité počas autorizácie užívateľov. Parametre sa nastavujú do novo vytvoreného súboru s názvom **config.yaml**.


```
APP:
  FLASK_APP: wsgi.py
  FLASK_ENV: production
  SECRET_KEY: <secret_key>
  DEBUG: False
  TESTING: False
  SQLALCHEMY_DATABASE_URI:
  postgresql://<username>:<passwd>@localhost:5432/<db_name>
  SQLALCHEMY_TRACK_MODIFICATIONS: False
GOOGLE_API:
  GOOGLE_CLIENT_ID: <google_client>
  GOOGLE_CLIENT_SECRET: <google_secret>
  GOOGLE_DISCOVERY_URL: <google_url>
```

Následne musíme vytvoriť novú rolu a databázu. To je možné vykonať následným sledom príkazov. Kde bude vytvorená nová rola s názvom **verifier** a s databázou **covidpass_verifier**. Následne nato bude vytvorená tabuľka zadáním názvu funkcie **create_db**. Na samom konci sledu je vykonaná kontrola prítomnosti novej tabuľky.

```
(venv)$ sudo -u postgres psql
postgres=#CREATE ROLE 'verifier' WITH LOGIN ENCRYPTED PASSWORD
'verifier';
postgres=#CREATE DATABASE covidpass_verifier;
(venv)$ python3 manage.py create_db
(venv)$ sudo -u postgres psql -d covidpass_verifier
postgres=# \dt
```

Pre jednoduchšie ovládanie aplikácie, bude pridaná do systému ako služba, ktorá bude ovládaná pomocou **systemctl**. Ako prvé je potrebné nastaviť konfiguráciu novej služby do súboru, ktorá bude službu zastupovať.

```
$ sudo nano /etc/systemd/system/web-verifier.service
```

Do súboru bude pridaná konfigurácia, ktorá sa nachádza v koreňovom súbore projektu nazývaným **web-verifier.service**. Po tomto nastavení je nutné obnoviť systém - to musí byť vždy vykonané po zmene. Následne bude služba spustná.

```
$ sudo systemctl daemon-reload
$ sudo systemctl start web-verifier.service
```

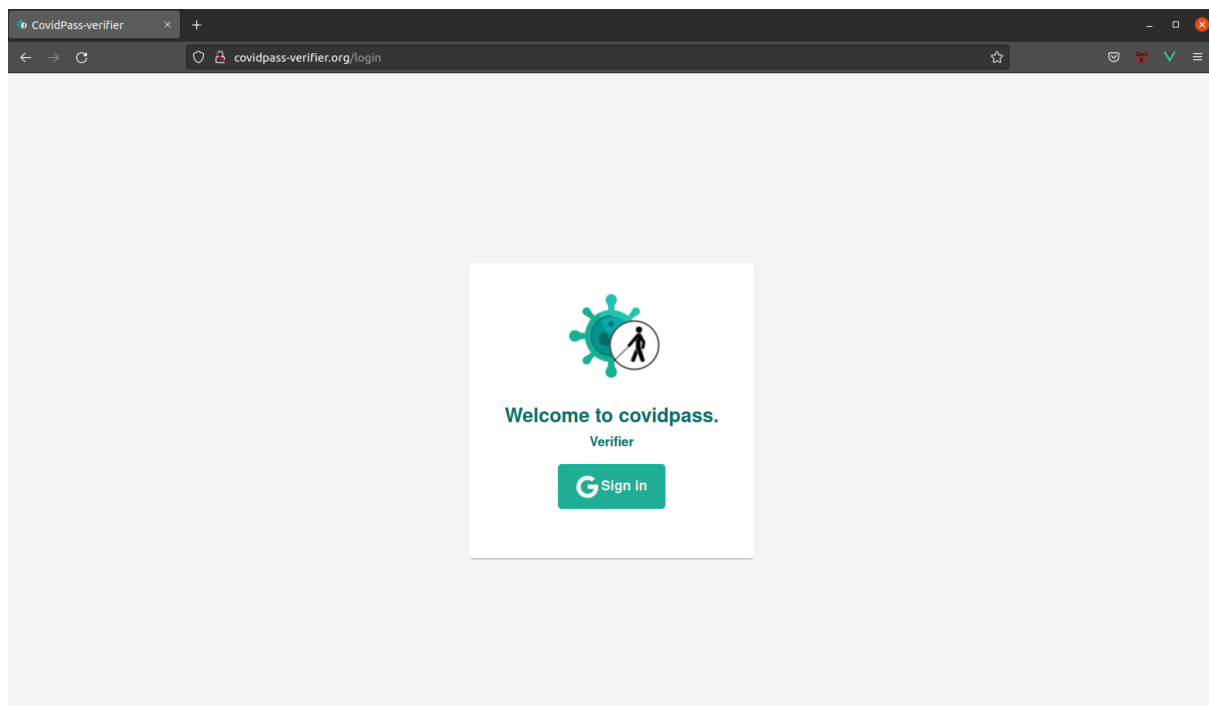
Nastavenie webového prehliadača

Pred samotným nastavením prehliadača, je potrebné pridať riadok do súboru `/etc/hosts`. Dôvodom pridania, je že aplikácia autorizuje pomocou Googlu, ktorý umožňuje použiť `localhost`, alebo doménové meno. Aplikácia beží na porte 8001 a nazvaná bude ako `covidpass-verifier.org`.

```
192.168.6.6:8001 covidpass-verifier.org
```

Následne je nastavené **http proxy** vo webovom prehliadači Firefox obdobne ako pri aplikácii vydavateľa - rozdielny port.

Týmto sa nastavili všetky potrebné nastavenia k spusteniu aplikácie overovateľa. Úvodná stránka žiada užívateľa o autentizáciu, kde po stlačení tlačítka bude presmerovaný smerom k googlu.



Po úspešnom autorizovaní je užívateľovi zobrazená stránka s názvom **dashboard**. Skladá sa z troch častí. Prvá je hlavička obsahujúca logo a tlačidlo slúžiace k odhláseniu. V strede sa nachádza tabuľka obsahujúca logovacie záznamy získané z procesu overenia - tieto dáta sú fiktívne a nadefinované na koncovom bode. Na pravej časti je vyobrazený box s dvoma typmi tlačidiel. Prvým je možnosť **options** umožňuje spustenie a vypnutie skriptu na overenie digitálnych certifikátov - funkčnosť bola otestovaná na ovládanie služby apache. Druhé tlačidlo má podobu ikony, ktoré po stlačení zobrazí sidebar

obsahujúci voliteľné parametre na základe, ktorých bude systém overovať

The screenshot shows the CovidPass-verifier dashboard. The main section displays a table of logs with columns for Time-stamp, Verify, and Attributes. The table contains 10 rows of data. To the right, there is a 'Manage s' panel with a list of attributes that can be selected or deselected. The 'Attributes' panel is currently open, showing a list of attributes with checkboxes. The 'Save' button is at the bottom of the panel.

| Time-stamp | Verify | Attributes |
|-------------------------|-----------|---|
| 2022-05-09 20:30:16.945 | VERIFY_OK | ["Cheat", "Cert", "Attribute 11", "Attribute 13"] |
| 2022-05-09 20:30:20.945 | VERIFY_OK | ["Cheat", "Cert", "Attribute 11", "Attribute 13"] |
| 2022-05-09 20:31:00.945 | VERIFY_OK | ["Cheat", "Cert", "Attribute 11", "Attribute 13"] |
| 2022-05-09 20:30:16.945 | VERIFY_OK | ["Cheat", "Cert", "Attribute 11", "Attribute 13"] |
| 2022-08-09 20:30:20.945 | VERIFY_OK | ["Cheat", "Cert", "Attribute 11", "Attribute 13"] |
| 2022-05-09 20:30:16.945 | VERIFY_OK | ["Cheat", "Cert", "Attribute 11", "Attribute 13"] |
| 2022-05-09 20:30:20.945 | VERIFY_KO | ["Cheat", "Cert", "Attribute 11", "Attribute 13"] |
| 2021-05-09 20:30:16.945 | VERIFY_OK | ["Cheat", "Cert", "Attribute 11", "Attribute 13"] |
| 2022-05-09 20:30:20.945 | VERIFY_KO | ["Cheat", "Cert", "Attribute 11", "Attribute 13"] |
| 2022-05-09 20:30:16.945 | VERIFY_OK | ["Cheat", "Cert", "Attribute 11", "Attribute 13"] |

Attributes management panel:

- ☒ Firstname
- ☐ Surname
- ☒ Birthdate day
- ☐ Birthdate month
- ☒ Birthdate year
- ☐ Hash of the photo
- ☒ Vaccine/prophylaxis
- ☐ Vaccine medical product
- ☒ Manufacturer
- ☐ Total number of doses
- ☐ Unique certificate identifier
- ☒ Vaccination day
- ☒ Vaccination moth
- ☐ Vaccination year
- ☐ Completed vaccination
- ☐ Dose number
- ☐ Certificate issuer
- ☒ EU Member state
- ☐ Optional1
- ☐ Optional2

Save