

Zakon o izmjenama i dopunama Zakona o trgovini

Tehničke upute za vjerodostojnu provjeru punoljetnosti kupca putem sustava e-Gradani

Poslovni kontekst

Zakonom o izmjenama i dopunama Zakona o trgovini (NN 59/2026) propisana je obveza trgovaca, osoba iz članka 5. podstavaka 1. i 5. Zakona o trgovini te internetskih platformi koje putem interneta prodaju alkoholna pića, pića koja sadrže alkohol i energetska pića da u svoje informacijske sustave implementiraju i koriste tehničko rješenje za vjerodostojnu provjeru punoljetnosti kupca, sukladno članku 11.a Zakona.

Provjera punoljetnosti provodi se putem informacijskog sustava **e-Gradani**, u skladu s propisima kojima se uređuje državna informacijska infrastruktura.

Prilikom internetske kupnje alkoholnih pića, pića koja sadrže alkohol i energetskih pića kupac je obavezan dokazati svoju punoljetnost korištenjem sustava **e-Gradani**.

Ako kupac odbije provjeru punoljetnosti, trgovci i internetske platforme (dalje u tekstu: web shop/platforma) dužni su uskratiti prodaju navedenih proizvoda.

Upis u evidenciju/registraciju u sustav e-Gradani

Web shop/platforma obvezni su upisati se u evidenciju pri Ministarstvu gospodarstva.

Svaki subjekt dužan je kod popunjavanja obrasca zahtjeva potvrditi da je registriran za obavljanje djelatnosti trgovine na malo putem interneta i/ili usluge informacijskog društva, u skladu s propisima kojim se uređuje elektronička trgovina te za prodaju alkoholnih pića, pića koja sadrže alkohol i energetskih pića.

Zahtjev za upisom u evidenciju podnosi se elektroničkim putem dostavom popunjenog obrasca isključivo u word ili editabilnom pdf formatu te mora sadržavati sljedeće podatke:

Podaci o poslovnom subjektu:

- naziv subjekta
- MBS / MBO / MIBPG
- OIB subjekta
- adresa i mjesto
- službeni naziv web shopa/platforme (naziv koji će biti prikazan korisniku u mobilnoj aplikaciji)
- link za web shop/platformu
- redirect URI(s) — URL(ovi) na koje će sustav preusmjeriti korisnika nakon uspješne provjere (npr. <https://www.vas-shop.hr/callback>)
- adresa e-pošte na koju će Ministarstvo pravosuđa, uprave i digitalne transformacije dostaviti **client_id**
- podaci kontakt osobe

Nakon uspješne registracije, web shop/platforma zaprimiti će:

- **client_id** — jedinstveni identifikator vaše trgovine u sustavu
- testni endpointi – URL sustava na testu
- produkcijski endpointi – URL sustava na produkciji

Dostava podataka

Podaci se prikupljaju slanjem popunjenog obrasca zahtjeva (word ili editabilni pdf format) putem adrese e-pošte: evidencija-trgovci@mingo.hr

Zahtjevi će se zaprimati kontinuirano, međutim, dinamika prosljeđivanja Ministarstvu pravosuđa, uprave i digitalne transformacije bit će jednom tjedno – petkom.

Zaštita podataka

Podaci dobiveni tijekom provjere punoljetnosti smiju se koristiti isključivo u svrhu trenutačne verifikacije te se moraju obrađivati u skladu s propisima o zaštiti osobnih podataka i pravilima korištenja informacijskog sustava e-Građani.

Tehničko rješenje

Tehničko rješenje za vjerodostojnu provjeru punoljetnosti kupca implementirano je putem informacijskog sustava **e-Građani**, odnosno njegove mobilne inačice (**m-Građani**), koja se integrira s web shopovima/platformama radi sprječavanja kupnje alkoholnih pića i pića koja sadrže alkohol i energetske pića osobama mlađim od 18 godina.

Rješenje funkcionira po principu jednostavne **DA/NE verifikacije**, pri čemu sustav web shop-u/platformi šalje isključivo potvrdu da je kupac punoljetan, bez otkrivanja identiteta, OIB-a ili drugih osjetljivih podataka kupca.

Koraci integracije na strani web shopa/platforme

1. Registracija web shopa/platforme

Prije same integracije, web shop/platforma mora biti registriran u sustavu. Za registraciju je potrebno dostaviti:

- Službeni naziv web shopa/platforme (za prikaz korisniku na mobilnoj aplikaciji)
- Redirect URI(s) — URL(ovi) na koje će sustav preusmjeriti korisnika nakon uspješne provjere (npr. <https://www.vas-shop.hr/callback>)

Adresu e-pošte na koju će Ministarstvo pravosuđa, uprave i digitalne transformacije dostaviti **client_id** i održavati komunikaciju tijekom procesa integracije i testiranja. Nakon registracije dobivate:

- **client_id** — jedinstveni identifikator vašeg web shop-a/platforme u sustavu
- pristup testnoj verziji aplikacije m-Građani
- podršku prilikom testiranja

2. Pokretanje provjere dobi (Authorization Request)

Kada korisnik želi pristupiti sadržaju koji zahtijeva provjeru dobi, web shop/platforma preusmjerava korisnikov browser na authorization endpoint:

```
GET /idp/authorize?response_type=code&client_id=<client-id>&redirect_uri=<redirect-  
uri>&scope=age.alcohol&state=7f3c9d2a1b8e4c6f91d0a5b3e7c2f8a1&nonce=4d9f1c0a7b3e8d6f2  
a91c5e0b7d3a9f1&code_challenge=15RAengqWrq0-  
mpwjqU00yB_nXM6Qb5YOCSi5IKGl2o&code_challenge_method=S256
```

Parametri:

Parametar	Opis
response_type	Uvijek code
client_id	Vaš dodijeljeni identifikator
redirect_uri	Mora odgovarati jednom od registriranih URI-ja
scope	age.alcohol za provjeru punoljetnosti
state	Nasumični string koji služi za zaštitu od CSRF napada — vratit ćemo ga natrag
nonce	Nasumični string koji će biti uključen u ID token — služi za zaštitu od replay napada
code_challenge	BASE64URL(SHA256(code_verifier)) — PKCE zaštita
code_challenge_method	Uvijek S256

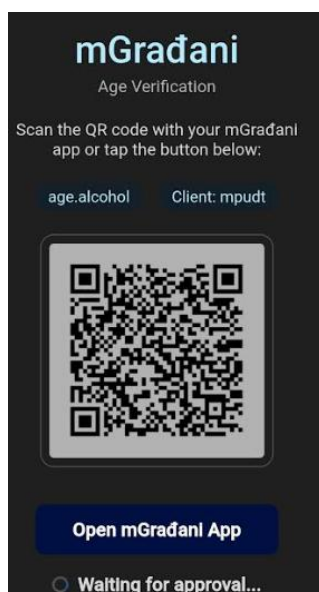
PKCE generiranje:

- Generirajte nasumični code_verifier (43–128 znakova, [A-Z, a-z, 0-9, -, _~])
- Izračunajte code_challenge = BASE64URL(SHA256(code_verifier))
- Spremite code_verifier za kasniju uporabu pri razmjeni tokena

3. Korisničko iskustvo

Nakon preusmjerenja, korisniku se prikazuje ekran za potvrdu identiteta putem mobilne aplikacije m-Građani. Korisnik pritiskom linka ili skeniranjem QR koda otvara mobilnu aplikaciju. Korisnik potvrđuje na mobitelu.

Prikazana stranica povlači status sesije. Nakon uspješne autentikacije radi redirect na web shop/platformu.



4. Primanje authorization code-a

Nakon što korisnik potvrdi na mobilnoj aplikaciji, browser se preusmjerava natrag na vaš `redirect_uri`:

```
GET https://www.vas-shop.hr/callback?code=AUTHORIZATION_CODE&state=ISTI_STATE_KOJI_STE_POSLALI
```

Obavezne provjere:

- Provjerite da state odgovara onom koji ste poslali u koraku 2
- Ako ne odgovara, odbacite zahtjev (moguć CSRF napad)

5. Zamjena code-a za token (Token Request)

Vaš backend šalje POST zahtjev na token endpoint:

```
POST /token Content-Type: application/x-www-form-urlencoded
grant_type=authorization_code&code=AUTHORIZATION_CODE&redirect_uri=https://www.vas-shop.hr/callback&client_id=VAŠ_CLIENT_ID&code_verifier=ORIGINALNI_CODE_VERIFIER
```

Važno: `code_verifier` mora biti isti onaj iz koraka 2 (prije hashiranja). Sustav verificira da `SHA256(code_verifier) = code_challenge` koji ste poslali pri autorizaciji.

6. Odgovor — ID Token

Uspješan odgovor sadrži:

```
{ "id_token": "eyJhbGciOiJSUzI1NiIs..." }
```

ID token je JWT (JSON Web Token) potpisan algoritmom RS256. Sadrži sljedeće relevantne claimove:

Claim	Opis
iss	Izdavatelj tokena (naš sustav)
aud	Vaš <code>client_id</code>
sub	Pseudonimni identifikator korisnika (pairwise — različit za svaki shop)
nonce	Isti nonce koji ste poslali u koraku 2
iat	Vrijeme izdavanja tokena
exp	Vrijeme isteka tokena
age.alcohol	true = korisnik je punoljetan, false = korisnik nije punoljetan

7. Validacija ID tokena

Vaš backend MORA provjeriti:

- 7.1. Potpis — verificirajte RS256 potpis tokena koristeći naš javni ključ (dostupan na JWKS endpointu)
- 7.2. `aud` — mora odgovarati vašem `client_id`
- 7.3. `nonce` — mora odgovarati onom koji ste poslali
- 7.4. token ne smije biti istekao
- 7.5. `iss` — mora biti očekivani izdavatelj

8. Odluka na temelju rezultata

```
if(id_token.age.alcohol == true) { // Korisnik je punoljetan — dopustite pristup } else { //  
Korisnik NIJE punoljetan — blokirajte pristup }
```

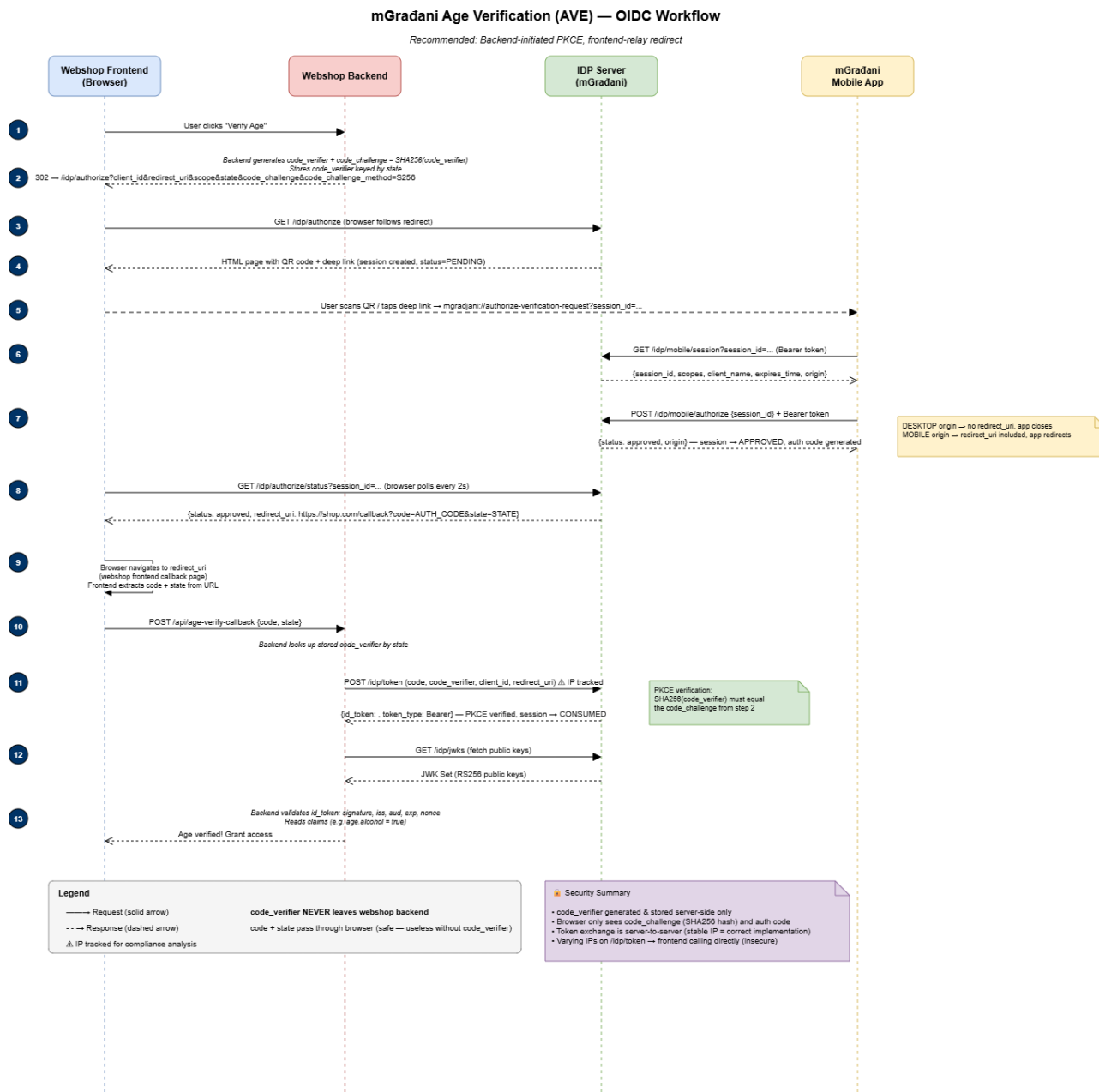
9. Sažetak poziva koje web shop mora implementirati

Korak	Tko	Što
1	Frontend	Redirect korisnika na /authorize s parametrima
2	Frontend	Primanje redirecta natrag s code i state
3	Backend	POST na /token s code + code_verifier
4	Backend	Validacija JWT potpisa i claimova
5	Backend/Frontend	Odluka o pristupu na temelju age.alcohol claima

10. Sigurnosna obavezna pravila

- Nikad ne šaljite code_verifier kroz browser - generiranje i razmjena tokena moraju ići preko vašeg backenda
- code_verifier generira backend
- code_verifier nikada ne smije biti vidljiv browseru
- code_verifier nikada ne smije biti spremljen u local storage
- code_verifier nikada ne smije biti poslan kroz URL
- Uvijek validirajte JWT potpis - ne vjerujte tokenu bez provjere
- Code je jednokratna - može se iskoristiti samo jednom
- Sub je pairwise pseudonim - ne možete identificirati korisnika, samo dobiti potvrdu dobi
- Ne pohranjujte osobne podatke - sustav vam ne šalje ime, OIB niti bilo koji drugi osobni podatak

Komunikacijski dijagram



Slika 1. Referentni tijek komunikacije između web trgovine, m-Građani sustava i mobilne aplikacije.

Testiranje i prelazak u produkcijski način rada

Potrebno je s e-mail adrese koju ste registrirali u Ministarstvu gospodarstva javiti e-mail adresu vašeg testera koja se koristi za prijavu na Google Play Store i/ili Apple Store koji će testirati uspostavljenu integraciju između vašeg web shopa i mobilne aplikacije m-Građani. Svaki web-shop smije prijaviti najviše jednog testnog korisnika. Taj e-mail prijavljen u jedan i/ili više mobilnih trgovina, biti će na određeno vrijeme (do produkcije) dodan kao testni korisnik aplikacije m-Građani (test) i na vašu e-mail adresu zaprimiti ćete od MPUDT:

- link na testni/e mobilne trgovine **m-Građani** i
- testne vjerodajnice za provjeru uspostavljene integracije i rad u aplikaciji m-Građani.

Nakon uspješno dovršenog procesa testiranja s vaše strane, s registrirane e-mail adrese šaljete službenu potvrdu o završetku testiranja i produkcijskoj spremnosti na određeni datum s vaše strane. Nakon toga, MPUDT će provesti potrebne aktivnosti za pripremu rada na produkcijskom okruženju sustava i aplikacije **m-Gradani**.

Upiti i kontakti

- Za pitanja iz poslovnog konteksta obratite se Ministarstvu gospodarstva na adresu e-pošte: evidencija-trgovci@mingo.hr
- Za tehnička pitanja i pitanja povezana s produkcijskim radom obratite se Ministarstvu pravosuđa, uprave i digitalne transformacije na adresu e-pošte: mgradjani@mpudt.hr