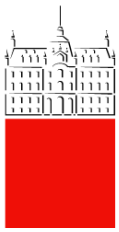
Univerza *v Ljubljani*



Uporabniška navodila za vzpostavitev MFA

Datum: 11. 9. 2023

Status dokumenta: Končni

Zadnja sprememba: Bartol, Klemen

Vsebina

Kazalo slik

1. Zgodovina različic dokumenta in povzetek

Verzija	Datum spremembe	Avtor
1.0	9. 6. 2023	Bartol, Klemen
1.1	31. 8. 2023	Žurbi, Rok
1.2	31. 8. 2023	Žurbi, Rok

Dokument se sprva osredotoči na razjasnitev pomembnosti uvedbe dodatnega varnostnega mehanizma - v splošnem na vse uporabniške profile, ki jih uporabljamo pri vsakodnevni uporabi aplikacij. V nadaljevanju pregledamo terminologijo in pojme, ki se tičejo teme. Nato pregledamo konfiguracijo avtentikacijske naprave za primer dodajanja multifaktorske avtentikacije ponudnika Microsoft in primer delovanja.

2. Uvod

V današnjem digitalnem svetu je varnost ključnega pomena za podjetja in njihove podatke. Vztrajno naraščajoče število kibernetskih napadov in kraje identitete predstavlja resno grožnjo za organizacije vseh velikosti. V tej situaciji je nujno zagotoviti učinkovite varnostne ukrepe za zaščito občutljivih informacij, kot so poslovni podatki, finančni podatki strank, intelektualna lastnina in drugi pomembni podatki.

Ena od ključnih metod za povečanje varnosti je uporaba multifaktorske avtentikacije (MFA). MFA je varnostni mehanizem, ki zahteva več kot en faktor preverjanja identitete pri dostopanju do računov in sistemov. Medtem ko tradicionalni načini avtentikacije, kot je uporaba samo gesel, postajajo vse manj zanesljivi, MFA omogoča podjetjem dodatno zaščito pred napadi in nepooblaščenim dostopom.

3. Terminologija

Za lažje razumevanje vsebine dokumenta definirajmo pojme, ki se bodo uporabljali v prihodnjih poglavjih.

Pojem	Razlaga
Avtentikacija	Overitev, preverjanje pristnosti ali avtentikacija je v računalništvu postopek, s katerim se strežnik prepriča, da je uporabnik zares tisti uporabnik, za kogar se predstavlja, da je. Najpogostejša metoda overjanja je vpis uporanbiškega imena in gesla pri postopku vpisovanja v določen IT sistem.
Avtentikacijska naprava	Naprava, ki jo bomo uporabljali za potrditev prijave. Najpogosteje je to mobilni pametni telefon, lahko pa tudi USB ključki (primer Gemalto).
Avtentikacijska aplikacija	Aplikacija, nameščena na pametnem telefonu, s katero potrjujemo novo prijavo.
Avtentikacijska metoda (način vpisa)	Avtentikacijska metoda je način avtentikacijskega varnostnega mehanizma, s katerim bomo potrjevali nove prijave svojega profila. Običajno so to načini: • potrjevanje prijave s pridobivanjem naključne številke po SMS na mobilni telefon • potrjevanje prijave s klicem in potrjevanjem prijave na mobilni telefon • potrjevanje prijave s klicem in potrjevanjem prijave na službeni telefon potrjevanje prijave z odobritvijo, poslano na predhodno vzpostavljeno avtentikacijsko aplikacijo na mobilnem pametnem telefonu
Multifaktorska avtentikacija (kratica MFA)	Multifaktorska avtentikacija je dodatni varnostni mehanizem, s katerim omogočimo svojim profilom višjo stopnjo varnosti. MFA je kratica v Mircosoftovem svetu, širše pa je znana tudi kot 2FA (dvofaktorska avtentikacija).
PIN številka	Štiri ali večmestna številka, ki lahko služi kot varnostni mehanizem kot alternativa geslu.

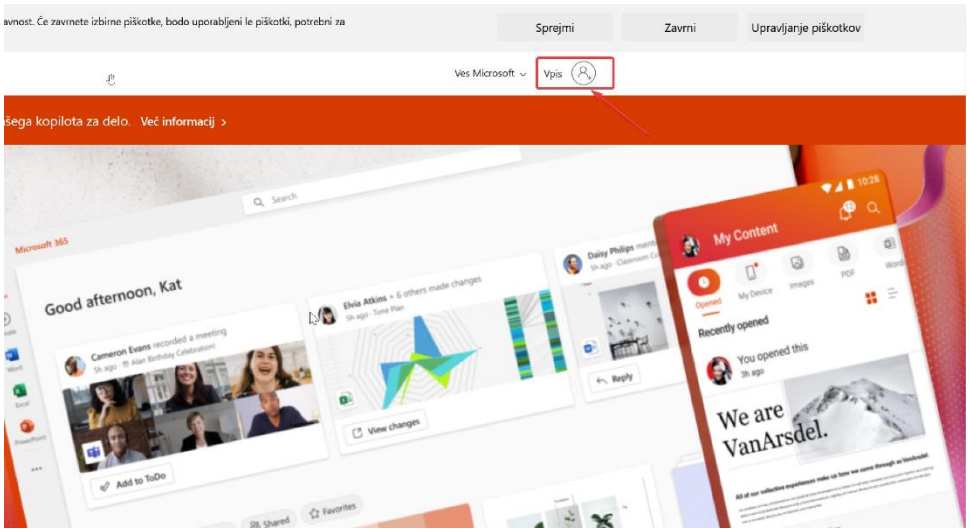
4. Vzpostavitev večfaznega potrjevanja

V nadaljevanju je predstavljena nastavitev MFA za službeni uporabniški račun. V predstavljenem primeru smo uporabljali mobilni pametni telefon z operacijskim sistemom Android in osebni računalnik, s katerim bomo dodajali varnostne mehanizme. V kolikor nimate pametnega mobilnega telefona, lahko uporabite navaden mobilni telefon (sms, klic) ali stacionarni telefon ali varnostni ključ.

Ko nastavite MFA vsaj enega od varnostnih mehanizmov, to sporočite računalniškemu centru, ki upravlja z uporabniškimi računi, da na vašem uporabniškem profilu aktivira potrjevanje preko MFA.

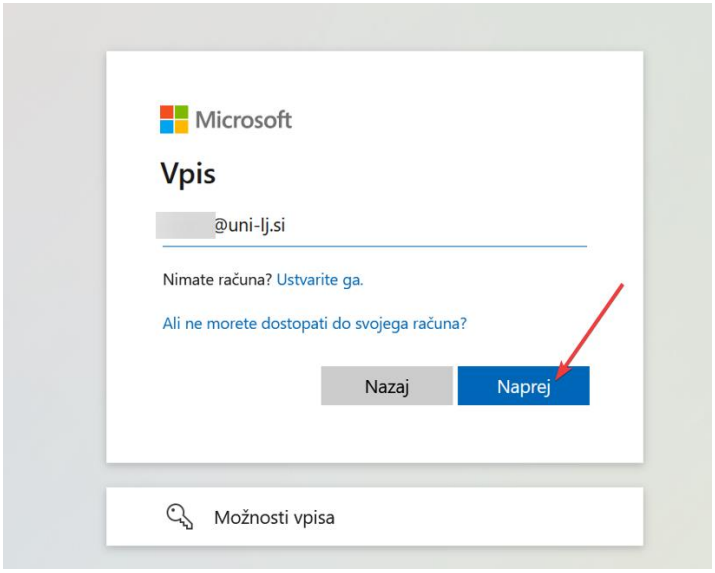
4.1.Dodajanje varnostnih mehanizmov na uporabniški profil

V izbranem spletnem brskalniku odpremo spletno stran Office.com in se prijavimo s svojim profilom (uporabniškim računom):



Slika 1: vpis v spletno stran office.com

Spletna stran nas preusmeri v prijavno okno, vpišemo svoje uporabniško ime in izberemo *Naprej*:

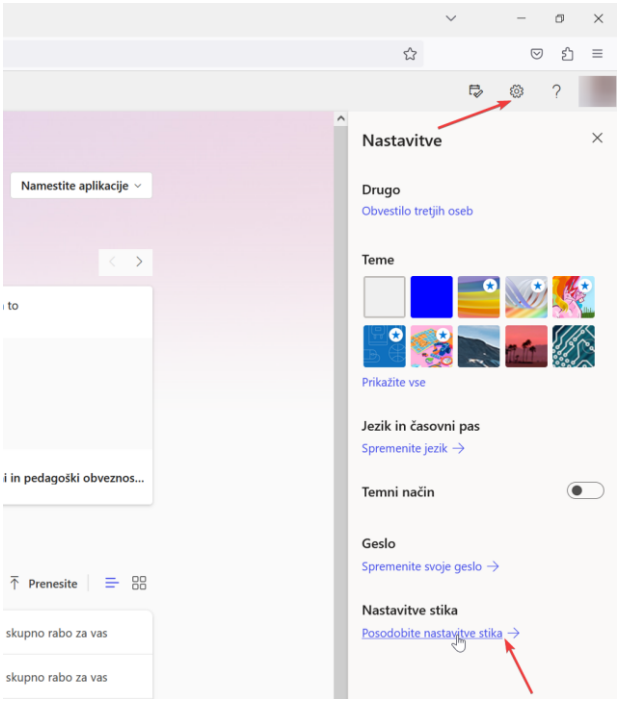


Slika 2: prijavno okno

Spletna stran nas ponovno usmeri na prijavno okno, vzpostavljenega za Univerzo v Ljubljani, kamor vpišemo uporabniško ime in geslo, ter izberemo *Naprej*:

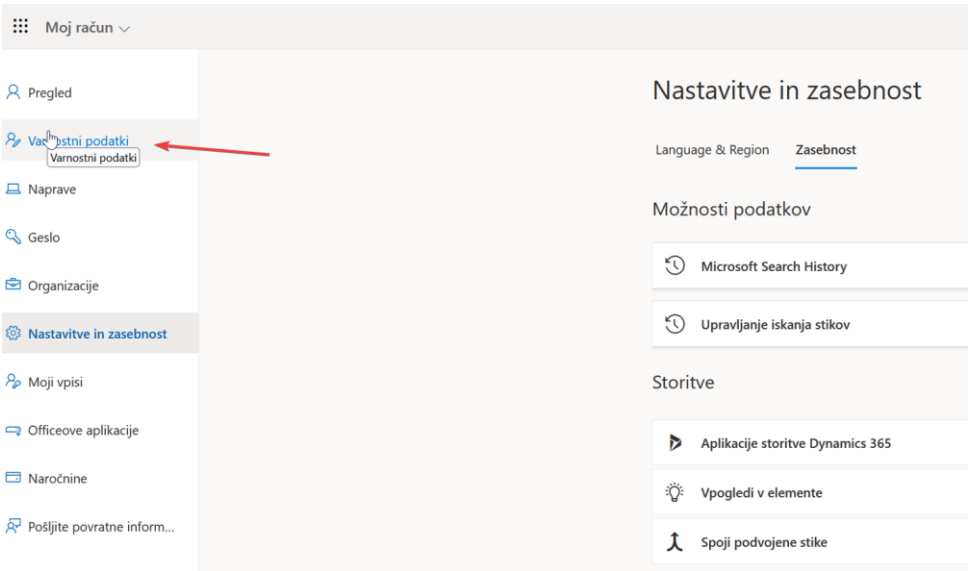
Slika 3: vnos podatkov v prijavno okno UL

Po uspešni prijavi se nahajamo na spletni strani, kjer izberemo *Možnosti* in nato *Posodobite nastavitve stika.*



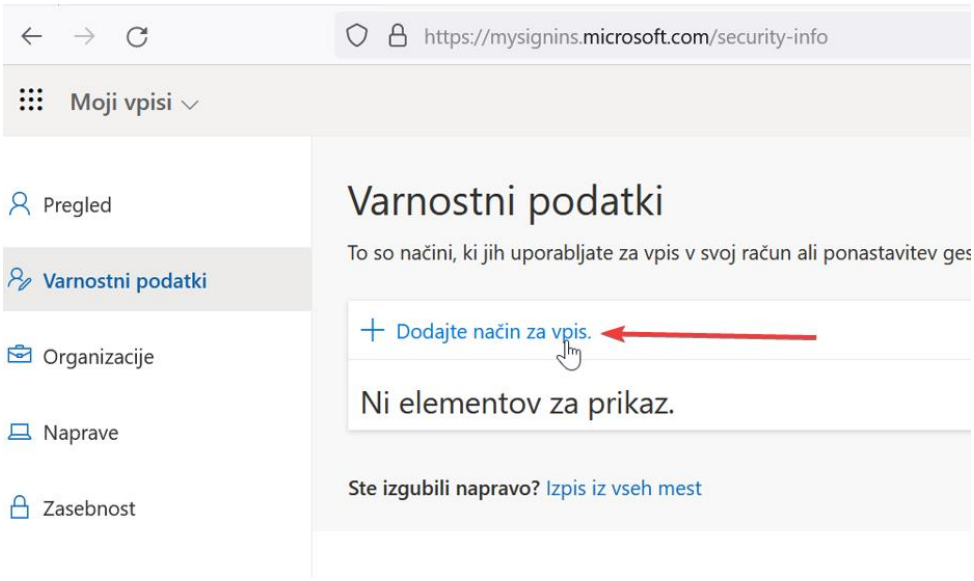
Slika 4: posodabljanje profila

Nato smo preusmerjeni na stran MyAccounts (v primeru, da nas ne preusmeri, prilagamo povezavo (https://myaccount.microsoft.com/settingsandprivacy/privacy) in izberemo *Varnostni podatki*:



Slika 5: rubrika varnostni podatki

Izberemo *Dodajte način za vpis*:



Slika 6: dodajanje avtentikacijske metode

Izbiramo lahko med več načini vpisa:

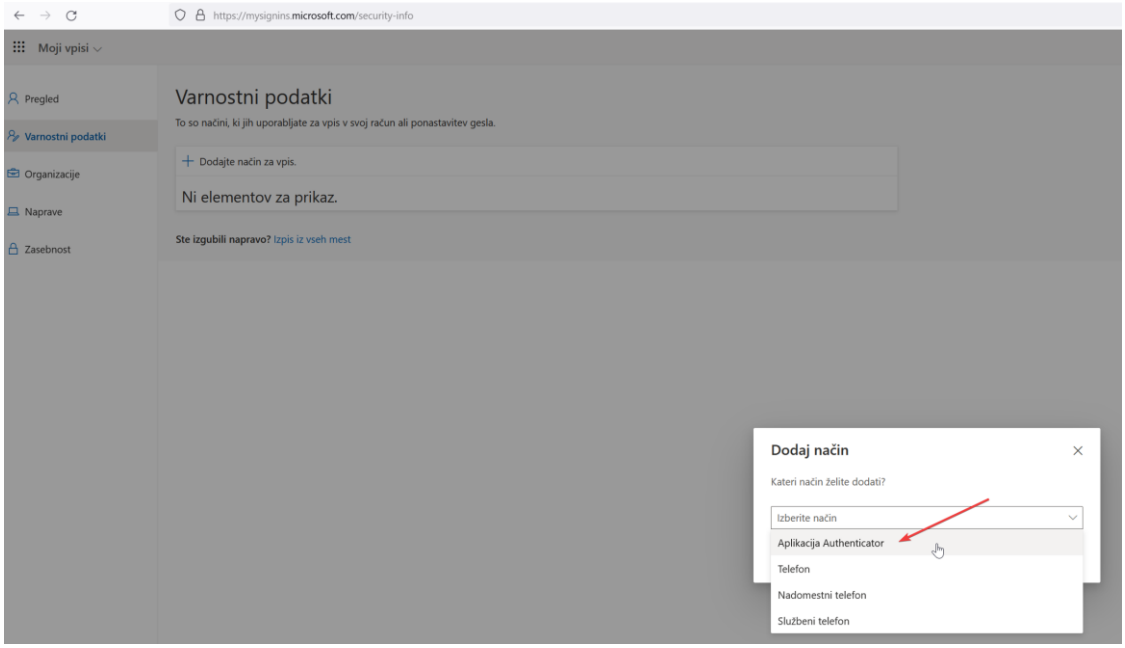
Aplikacija Avtentikator	Deluje na pametnem mobilnem telefonu Android, iOS	**Priporočljiv način**
Telefon	Koda preko SMS ali klic	Priporočamo kot **nadomestni način** ali namesto pametnega mob.
Nadomestni telefon	Koda preko SMS ali klic	Nadomestni način v primeru nezmožnosti uporabe os. telefona
Službeni telefon	Klic	Nadomestni način v primeru nezmožnosti uporabe os. telefona
Varnostni ključ	USB ključ, biometrično potrjevanje	Varnostni ključ mora biti ob vpisu vtaknjen v napravo.

NASVET: *priporočamo nastavitev vsaj dveh načinov. V primeru, da eden od načinov odpove, imate na voljo še druge. Na primer aplikacija Avtentikator + telefon (sms) na mobilno številko + nadomestni telefon (klic na službeno številko).*

Če ne uporabljate aplikacije Avtentikator, nastavite npr. sms/klic na mobilni telefon + klic na služben telefon.

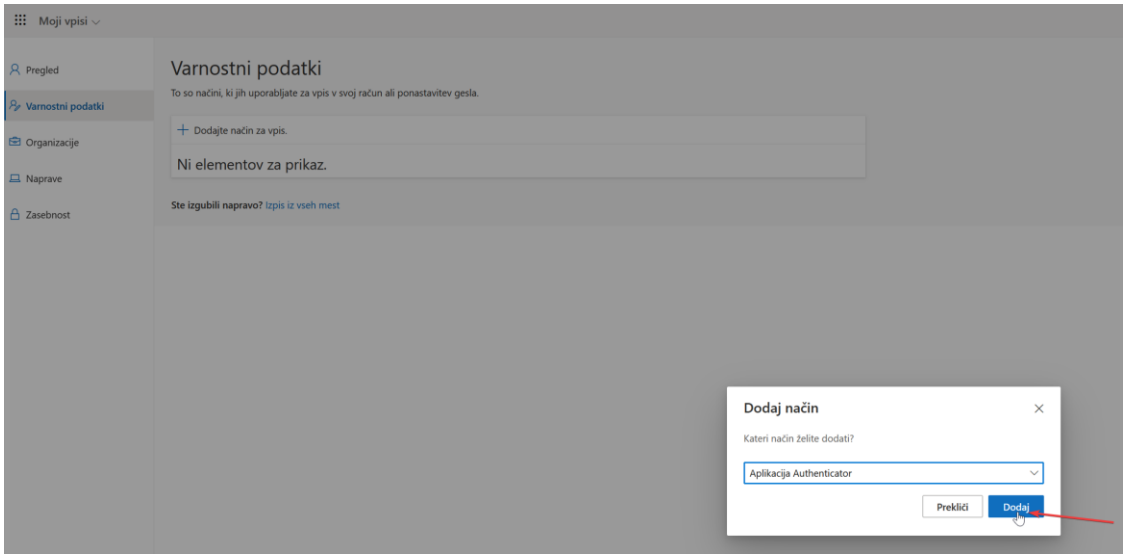
4.2.Nastavitev metode »Authenticator« na pametnem telefonu

Po izbiri *Dodajte način za vpis* na računalniku, se nam pojavijo vse možne avtentikacijske metode, ki jih lahko izberemo. Če želimo urediti avtentikacijo s pomočjo aplikacije Authenticator, izberemo možnost *Aplikacija Authenticator:*



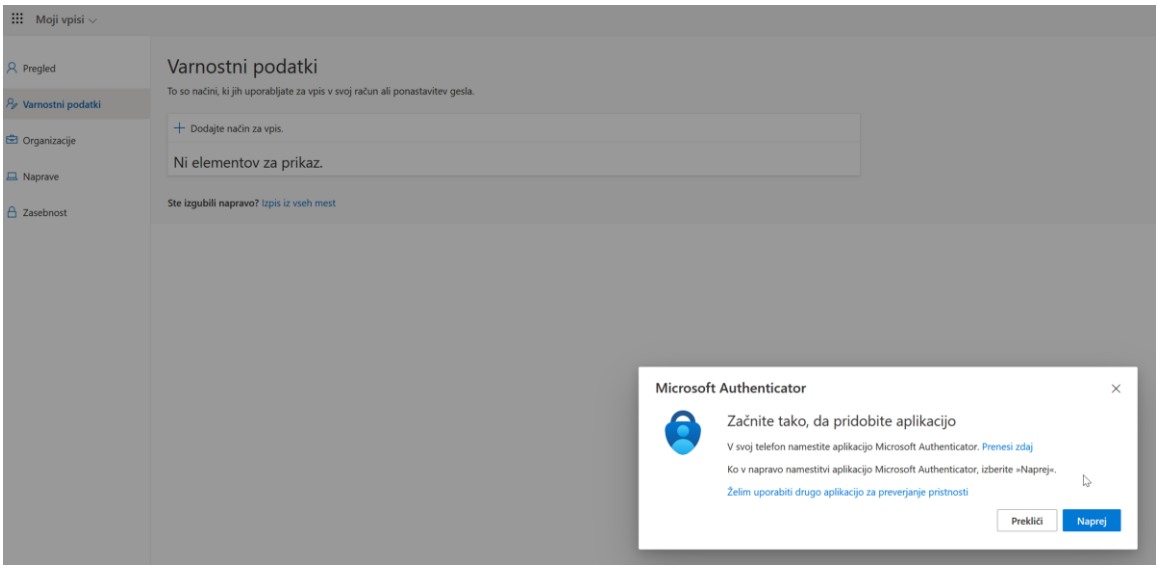
Slika 7: izbira možnosti Aplikacija Authenticator

In nadaljujemo z *Dodaj*:



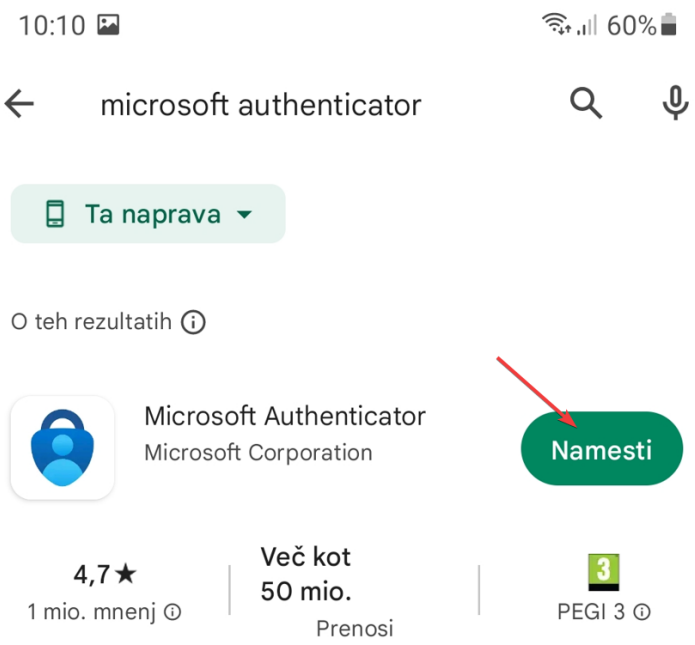
Slika 8: dodaj avtentikacijsko metodo

Na tej točki se nam pojavi naslednje okno:



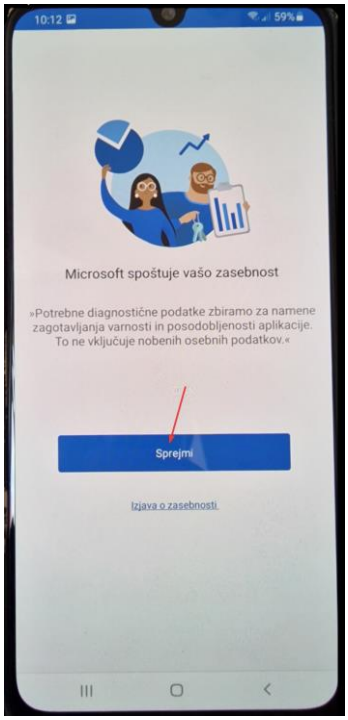
Slika 9: okno

Pustimo odprto okno na računalniku in vzamemo svoj **pametni mobilni telefon**, odpremo aplikacija *Trgovina Play* (*Play Store*) in poiščemo ter namestimo aplikacijo Microsoft Authenticator.



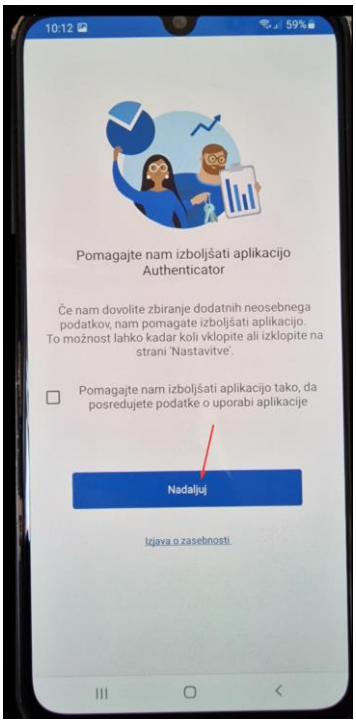
Slika 10: aplikacija Microsoft Authenticator

Po uspešni namestitvi aplikacijo jo odpremo in sprejmemo pogoje zasebnosti:



Slika 11: sprejmemo pogoje zasebnosti

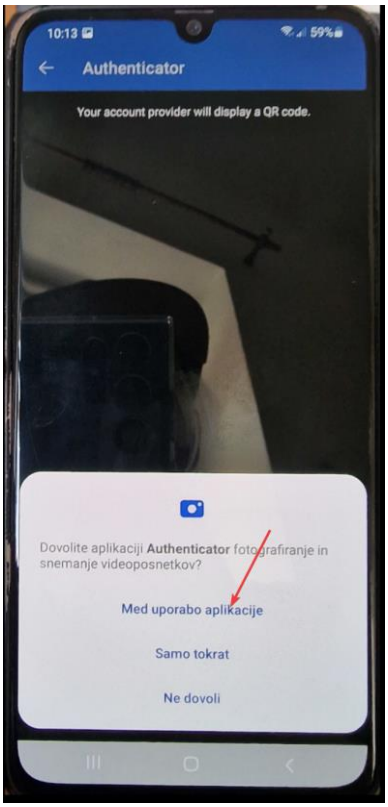
Pustimo odkljukano in izberemo *Nadaljuj:*



Slika 12: pustimo odkljukano in nadaljujemo

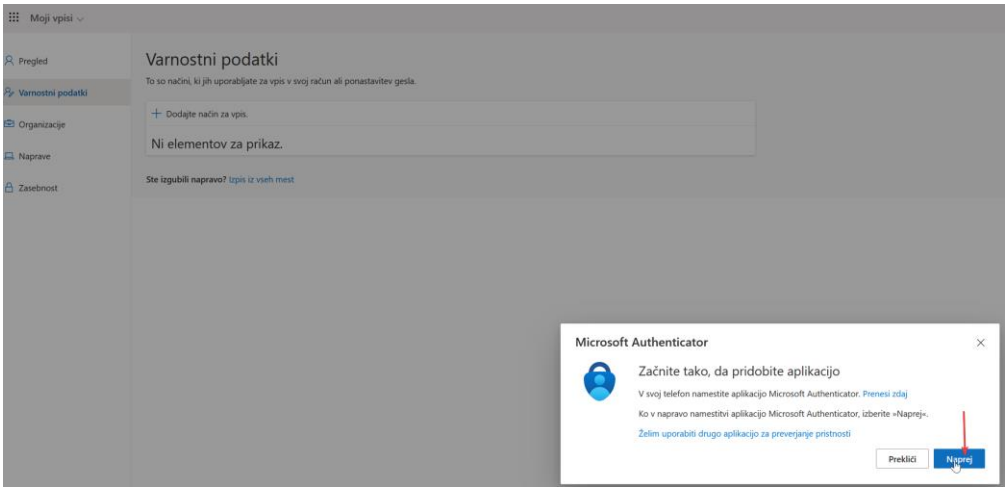
Izberemo možnost *Optično preberite kodo QR:*

Slika 13: korak optičnega prebiranja QR kode



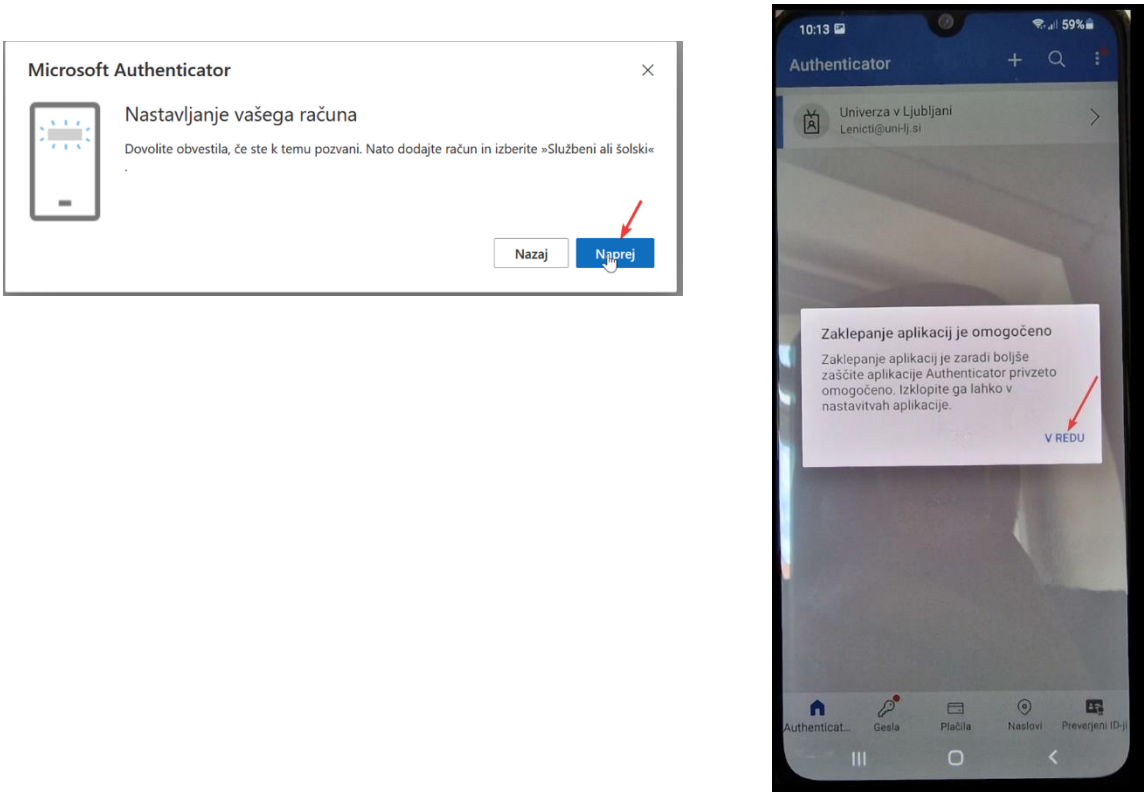
Slika 14: na mobilnem telefonu omogočimo dovoljenja

Gremo **nazaj na računalnik na še vedno odprto okno**, izberemo *Naprej* in se na monitorju pojavi QR koda. To QR kodo **optično preberemo s pametnim mobilnim telefonom:**



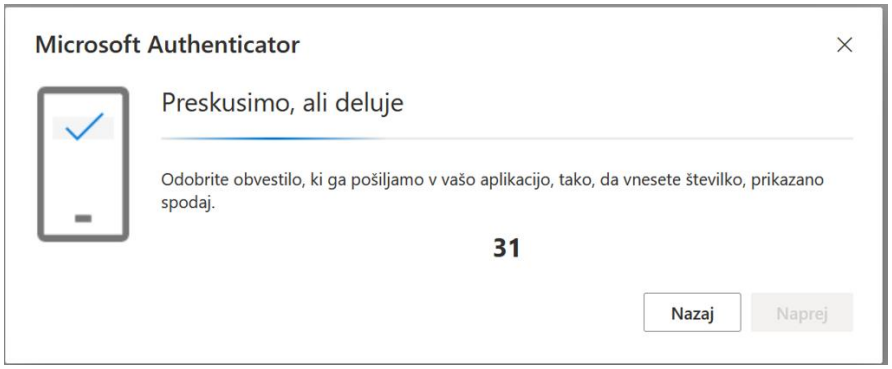
Slika 15: izbira Naprej

Na monitorju se pojavi QR koda. To QR kodo **optično preberemo s pametnim mobilnim telefonom.** Ko jo skeniramo na računalniku izberemo *Naprej,* **na pametnem mobilnem telefonu pa *V redu*.**

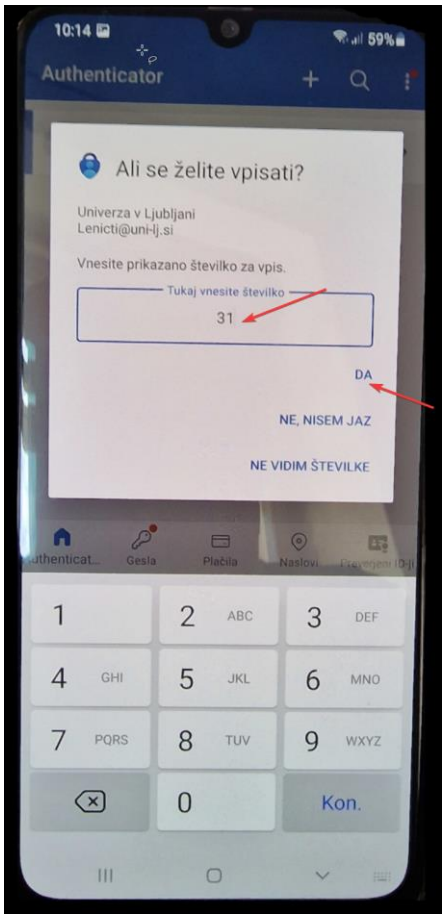


Slika 16: Avtentikator – dovoljenje za obvestila in zaklepanje aplikacije

Na **računalniku se pojavi številka**, ki jo vpišemo v aplikacijo na **pametnem mobilnem telefonu**:

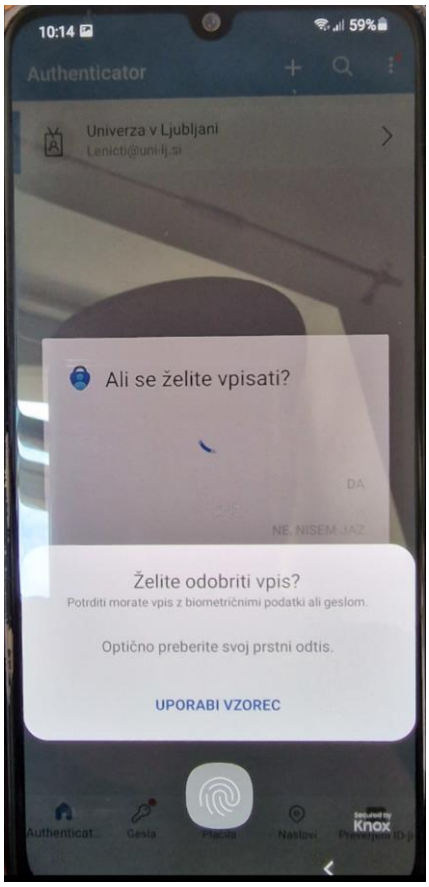


Slika 17: časovno omejena številka za vpis na pametnem mobilnem telefonu



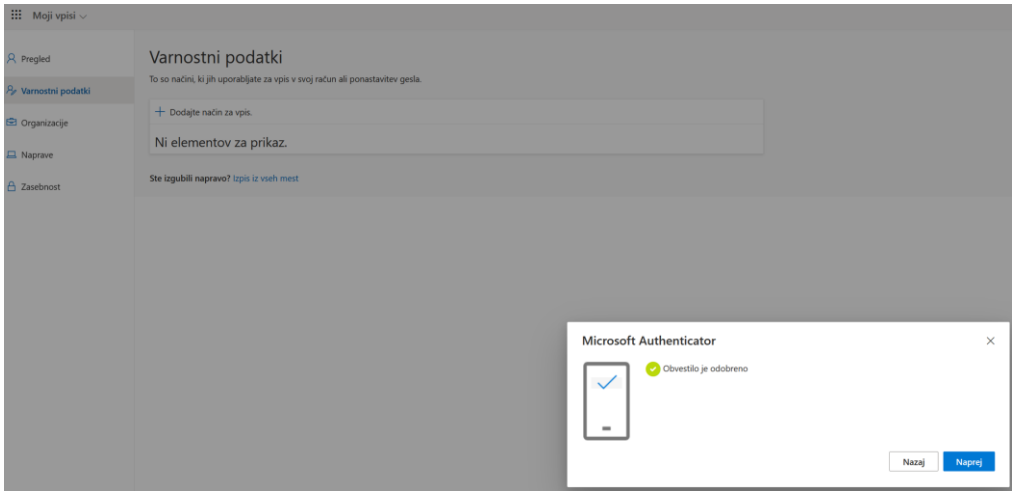
Slika 18: vpis številke iz računalnika in potrditev prijave z izbiro

Če imamo nastavljeno zaklepanje pametnega mobilnega telefona, moramo odobriti vpis z eno od predhodno nastavljenih varnostnih metod:



Slika 19: odobritev vpisa

Če smo naredili vse pravilno, smo o uspešnosti obveščeni na računalniku:

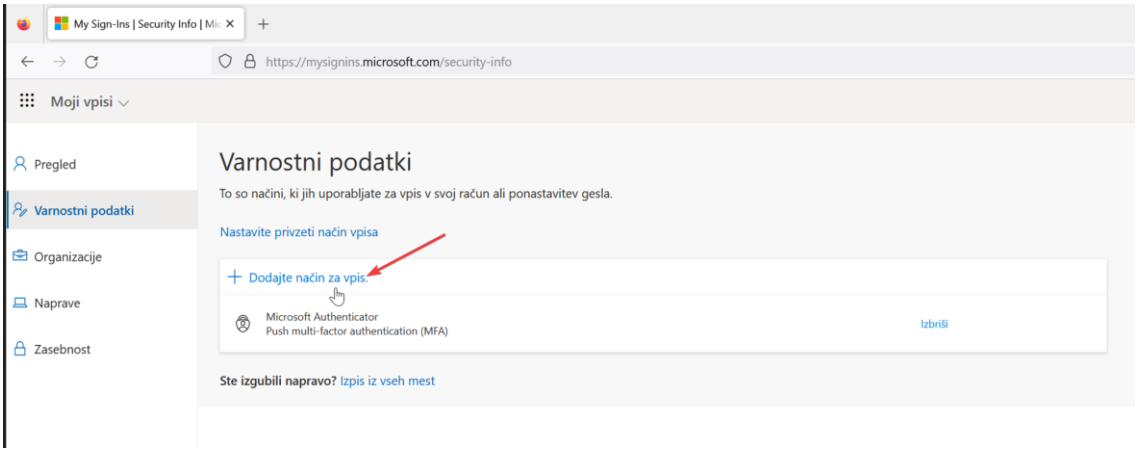


Slika 20: uspešno dodana avtentikacijska metoda

Na takšen način smo dodali avtentikacijsko metodo z uporabo aplikacije Authenticator. Če želimo dodati SMS ali kakšno drugo metodo, lahko nadaljujemo z nadaljnjim prebiranjem navodil.

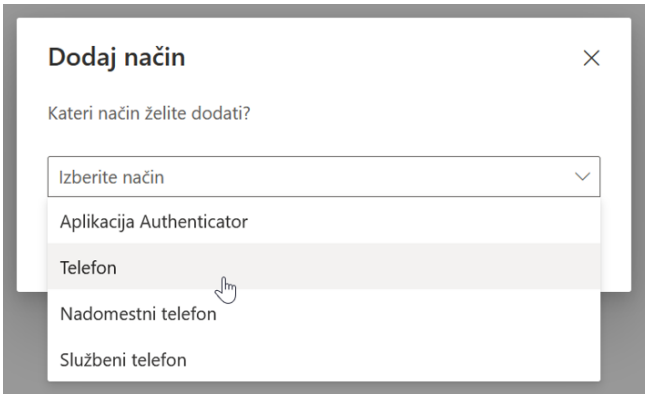
4.3.Nastavitev metode »mobilni telefon«

Nahajamo se na strani (https://myaccount.microsoft.com/settingsandprivacy/privacy) in izberemo *Dodajte način za vpis*:

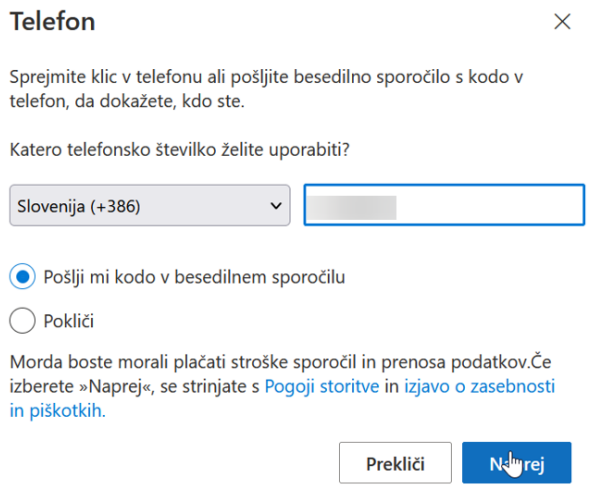


Slika 21: dodajte način za vpis

Izberemo opcijo *Telefon:*

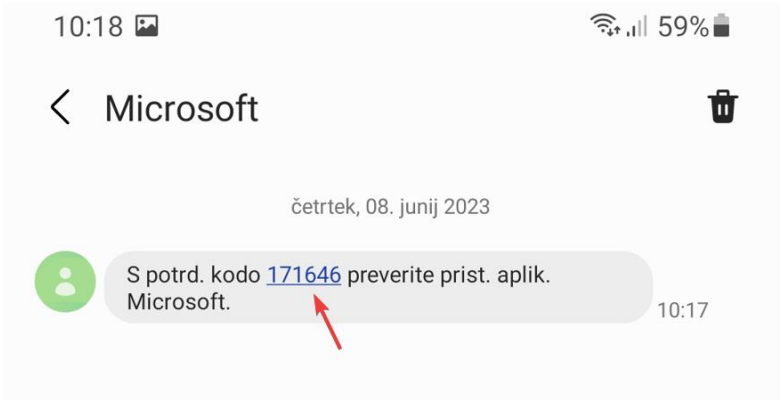


Slika 22: izbira Telefon

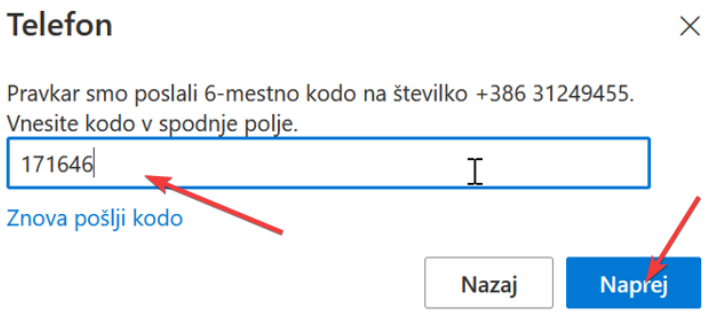


Slika 23: vpišemo svojo številko in izberemo Naprej

Vzamemo mobilni telefon, počakamo na prejeto SMS sporočilo in v okno v računalnik prepišemo 6-mestno, časovno omejeno številko:

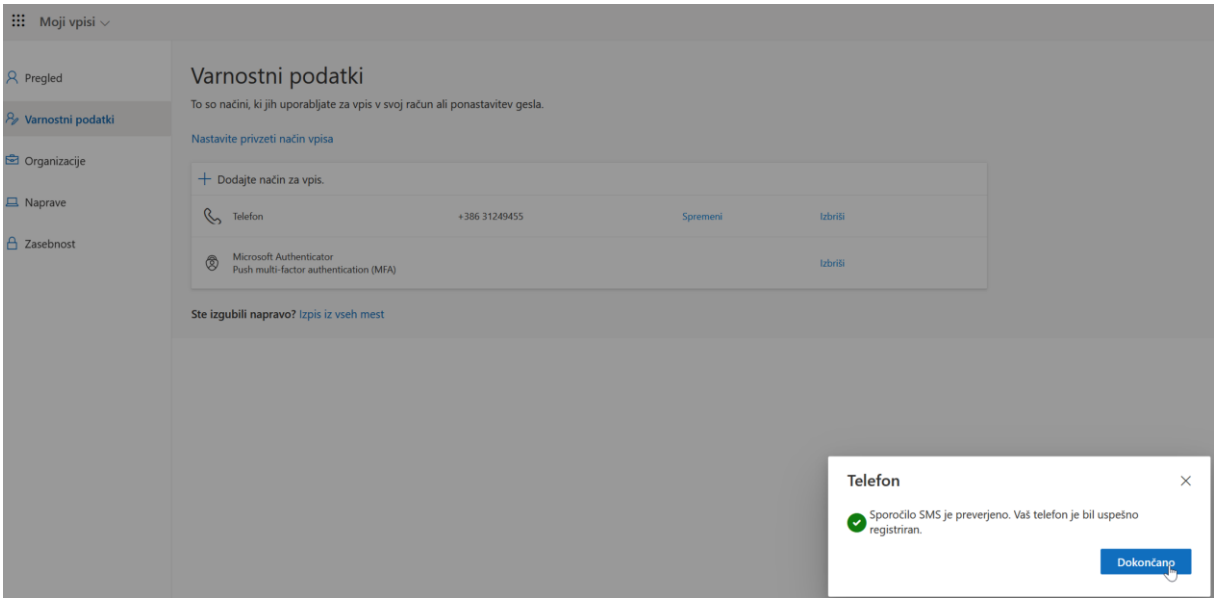


Slika 24: prejeta 6-mestna, časovno omejena številka



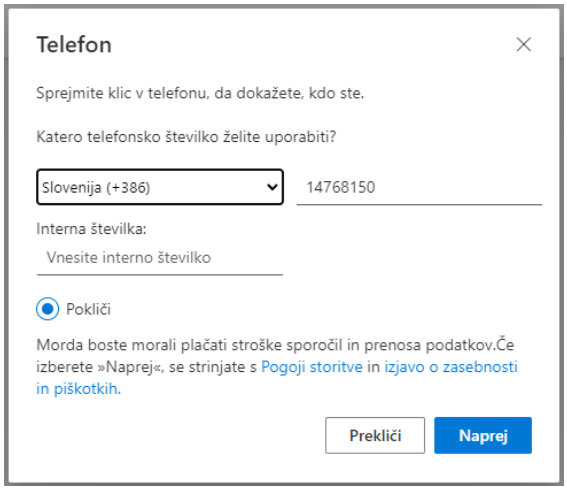
Slika 25: vpis številke v prikazano okno na računalniku

Če smo vpisali pravilno 6 mestno kodo, dobimo potrdilo o uspešnosti dodane avtentikacijske metode:



Slika 26: uspešno dodana avtentikacijska metoda

Na enak način lahko nastavite tudi *Nadomestni telefon, Službeni telefon.* Pri slednjem je na voljo zgolj klic. Vpišite vašo službeno številko, polje *interna številka* pustite prazno.

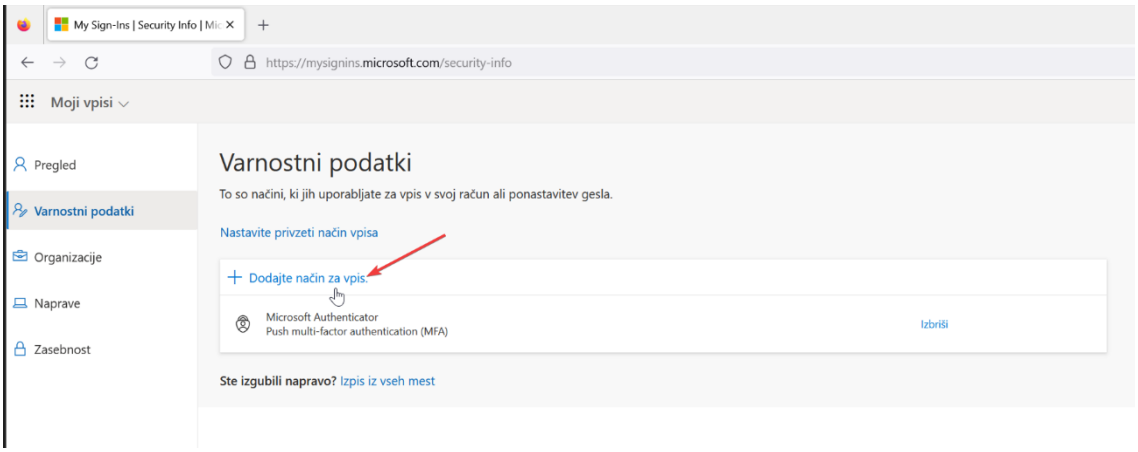


Slika 27: Vpis številke za Službeni telefon

4.4.Nastavitev metode »varnostni ključ«

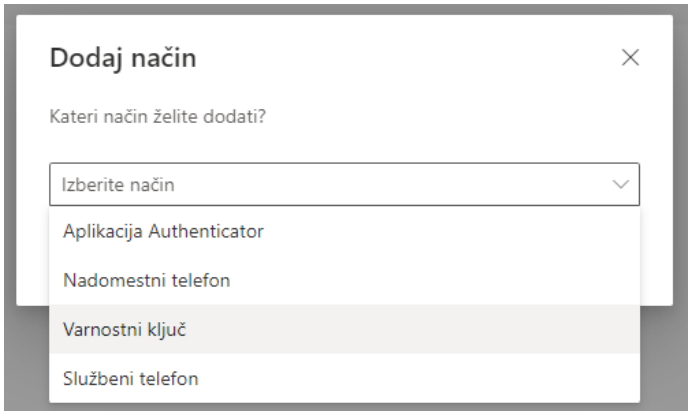
Pri tem načinu boste potrebovali varnostni ključek, ki ustreza standardu FIDO2. Za ključek se obrnite na vašo Službo IKT. **Predhodno si nastavite** način potrjevanja s telefonom ali *Avtentikator* aplikacijo!

Pojdite na https://myaccount.microsoft.com/settingsandprivacy/privacy in izberite *Dodajte način za vpis*:



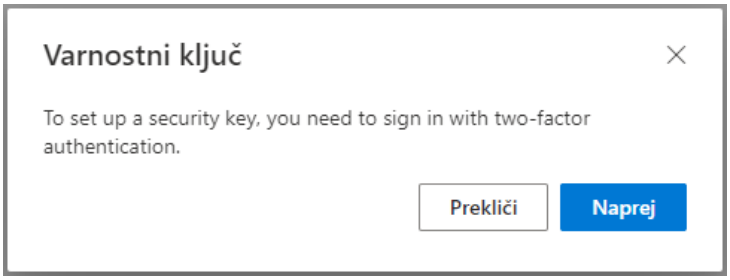
Slika 28: dodajte način za vpis

Izberite opcijo *Varnostni ključ:*



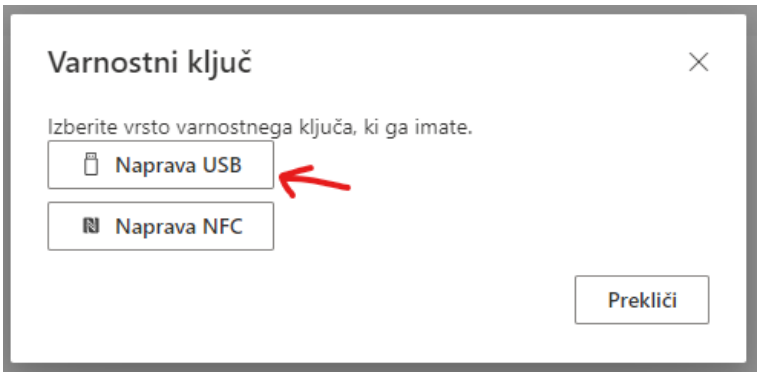
Slika 29: izbira Varnostni ključ

Potrdite izbiro *Varnostni ključ*.



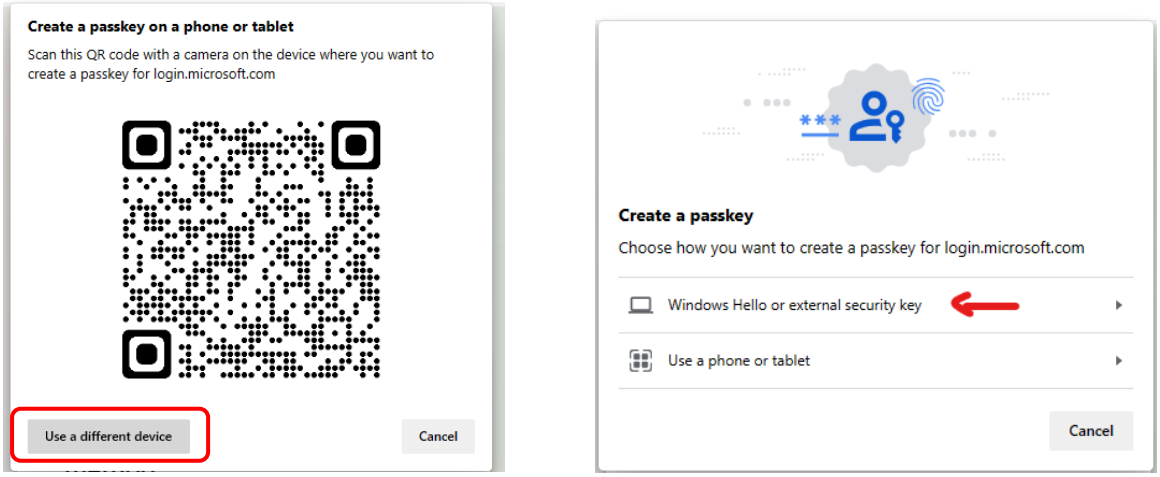
Slika 30: izbira Varnostni ključ

Kot vrsto ključa izberite »Naprava USB«



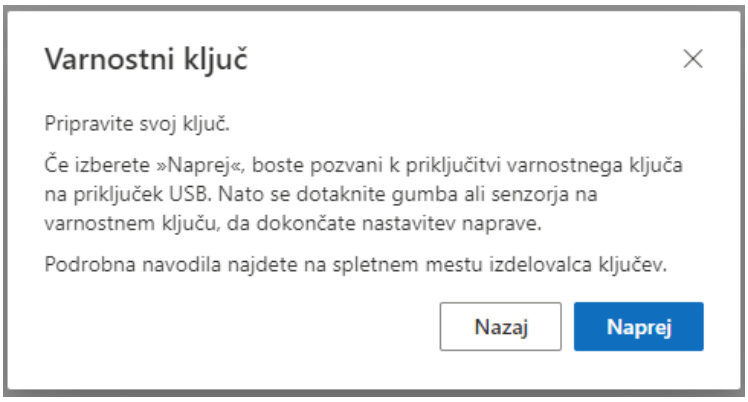
Slika 31: izbira tipa ključa - USB

Če se v naslednjem koraku pojavi QR koda, izberite »Uporabi drugo napravo« in v naslednjem koraku izberite »Uporabi Windows Hello ali zunanji varnostni ključ« (Slika 32).

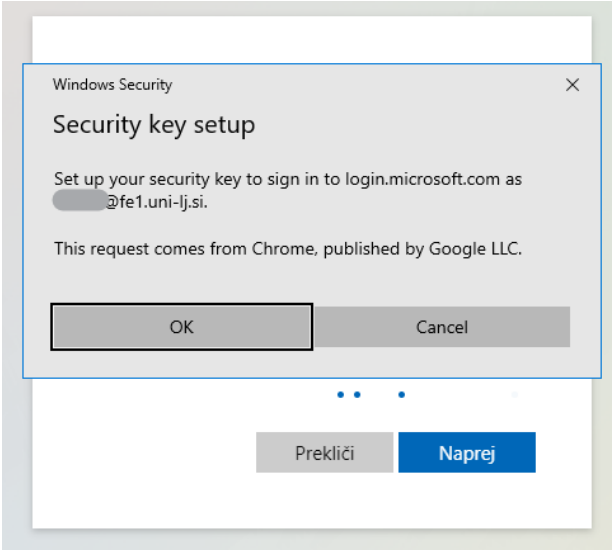


Slika 32: Izbira pravilne naprave

Nadaljujte s klikom Naprej.

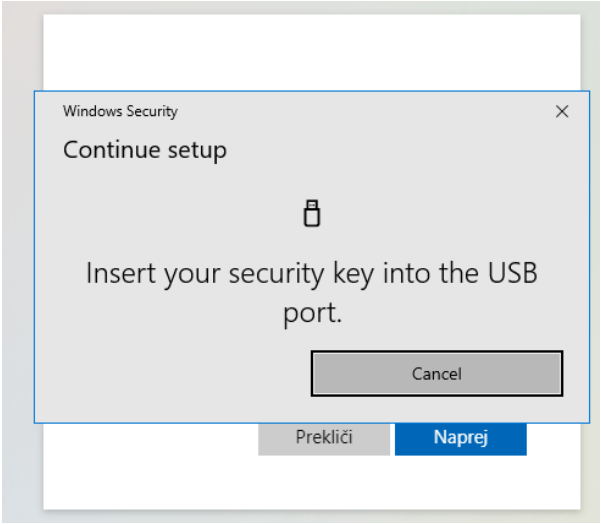


Slika 33: potrditev nadaljevanja namestitve



Slika 34: vezava prijave s ključem na uporabniški profil

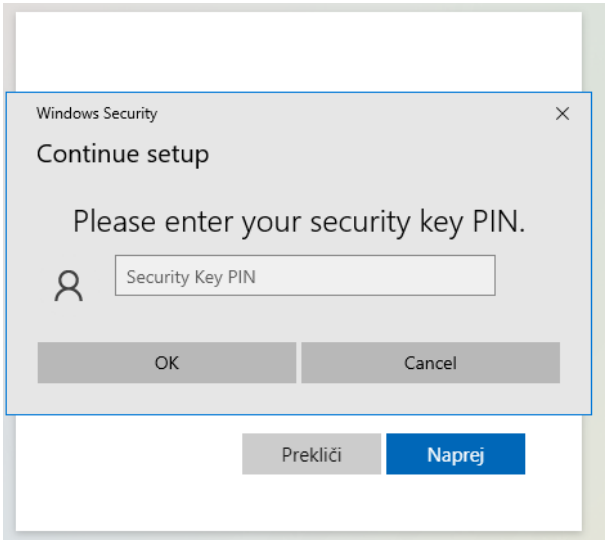
Pripravite varnostni ključ in ga ob sporočilu vtaknite v USB režo.



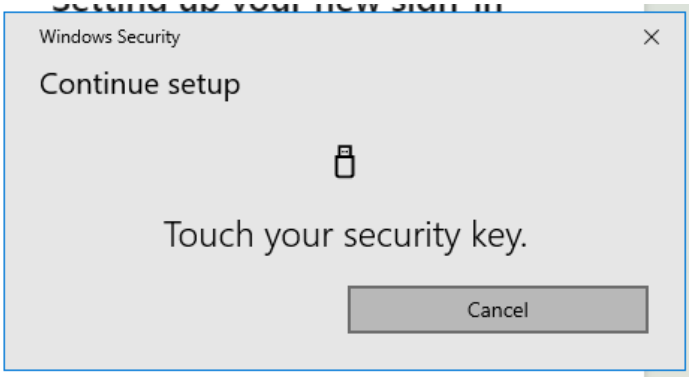
Slika 35: vstavitev ključa v USB režo

Ob prvi uporabi ključa, boste pozvani k **nastavitvi** PIN kode in biometričnega prstnega odtisa.

Ob naslednjih uporabah boste pozvani k vnosu PIN kode in prstnega odtisa.

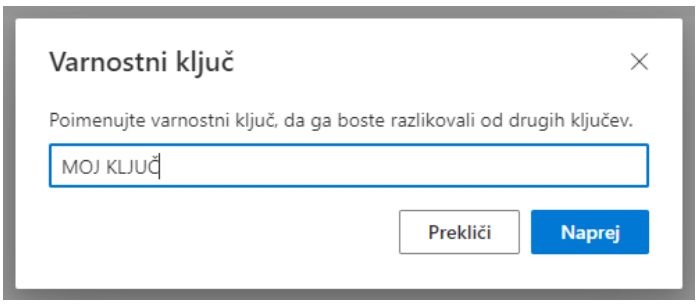


Slika 36: nastavitev PIN-a (samo prva aktivacija) ali vpis PIN-a



Slika 37: potrditev s prstnim odtisom

V zadnjem koraku le še poimenujete vaš ključ in postopek je zaključen.

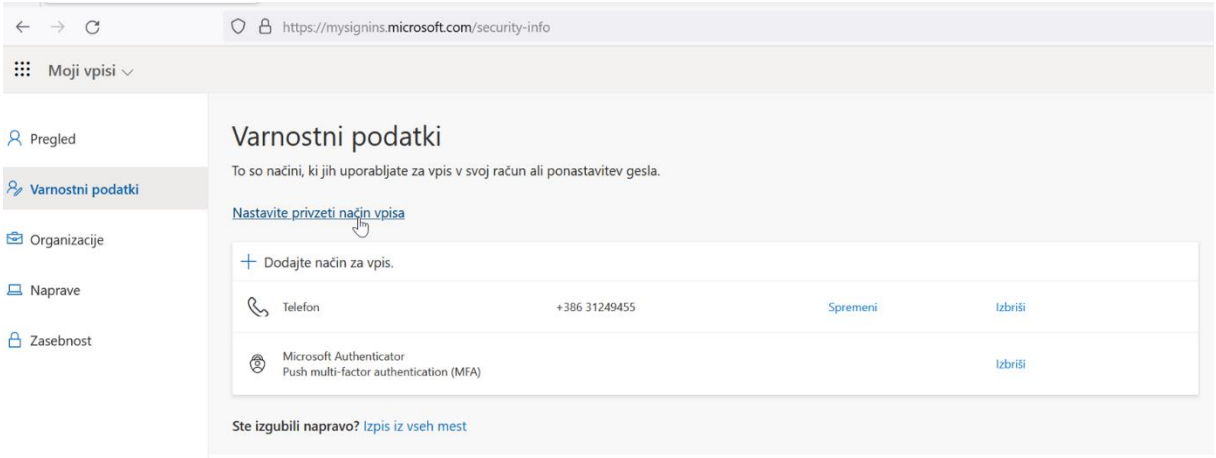


Slika 38: poimenovanje ključa

4.5.Spreminjanje privzetega načina avtentikacije

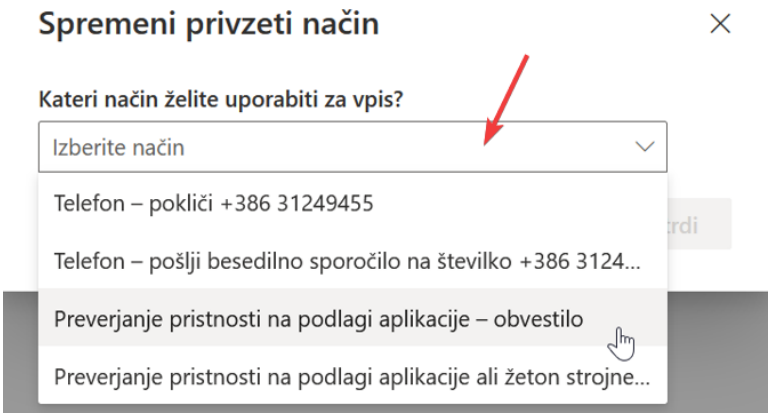
Nastavljene metode avtentikacij za naš profil, lahko vidimo na spletni strani (https://mysignins.microsoft.com/security-info), kjer lahko **spremenimo privzeti način** vpisa. Privzeti način se bo uporabljal kot prva ponujena, t.j. prednostna metoda potrjevanja. **Vsekakor lahko ob vsakem vpisu vedno izbiramo tudi med drugimi načini, ki smo jih predhodno nastavili.**

Privzeto avtentikacijsko metodo nastavimo takole:



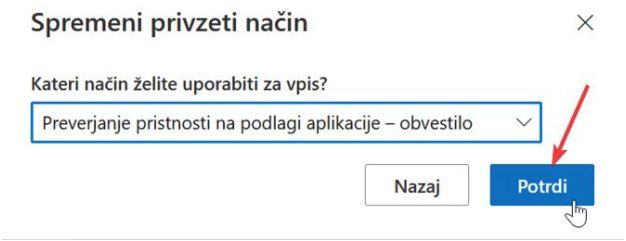
Slika 39: privzeti način vpisa

Preko spustnega menija izberemo način:



Slika 40: izbira načina

In potrdimo izbiro:

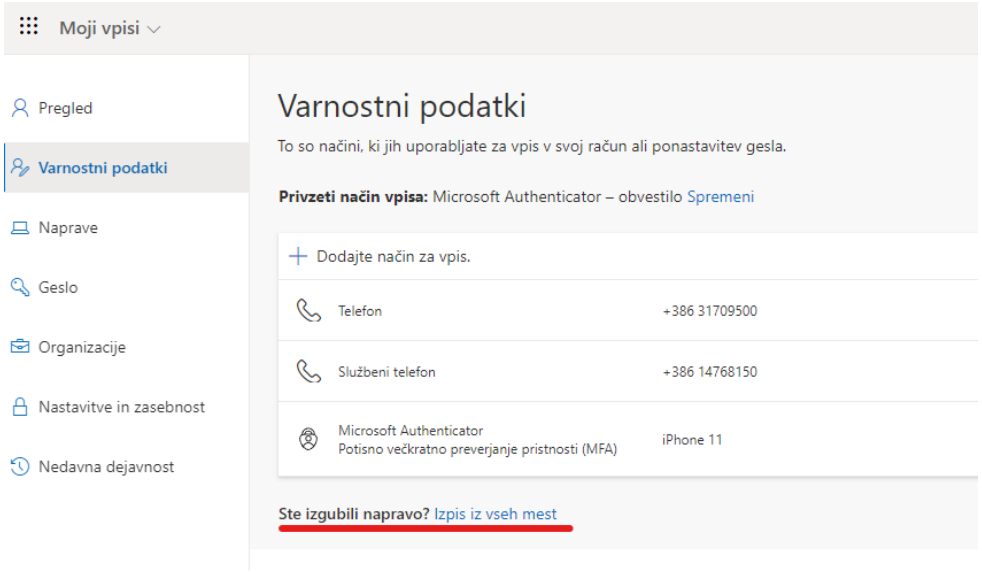


Slika 41: potrjevanje avtentikacijske metode

Na tej točki sporočite Službi IKT na članici, da ste dodali avtentikacijske metode in bi želeli uporabljati MFA. Ko Služba za IKT sporoči, da je MFA aktiviran, se bo ta poslej zahteval v prijavah z vašim uporabniškim računom[1].

4.6.Ukrepanje v primeru izgube ali odtujitve naprave

Če ste napravo, ki jo uporabljate za vpis – MFA izgubili ali vam je bila ukradena, se s klikom na »Izpis iz vseh mest« izpišite iz naprav in kontaktirajte Službo za IKT.



Slika 42: Izpis v primeru izgube naprave

5. Koristne povezave

1. Video navodila za vzpostavitev MFA: https://www.youtube.com/watch?v=VwEd-vhmVzI
2. Varnostni podatki: https://mysignins.microsoft.com/security-info
3. Microsoft 365 glavna stran: https://office.com/

[1] Nekatere aplikacije in storitve na UL trenutno še ne zahtevajo MFA.