SI-TRUST
Državni center za storitve zaupanja

SMERNICE ZA UPORABO IN INTEGRACIJO GRADNIKOV SISTEMA SI-PASS

Ministrstvo za digitalno preobrazbo
Državni center za storitve zaupanja

2024

Namen dokumenta:	Smernice podajajo najpomembnejše informacije v zvezi z gradniki sistema SI-PASS. Namenjene so vsem tistim, ki se ukvarjajo z avtentikacijo in elektronskim podpisovanjem v okviru svojih spletnih storitev (tako ponudnikom storitev kot razvijalcem)
Ciljne javnosti:	Skrbniki spletnih storitev, razvijalci informacijskih sistemov, rešitev in aplikaciji
Status:	Javno
Verzija:	1.0
Datum verzije:	22. 1. 2024
Avtorji:	Projektna skupina Državnega centra za storitve zaupanja

Zgodovina verzij

Datum	**Verzija**	**Sprememba**

Kazalo vsebine

Kazalo tabel

Kazalo slik

Kratice v dokumentu

Kratica	Naziv
eIDAS	UREDBA (EU) št. 910/2014 EVROPSKEGA PARLAMENTA IN SVETA z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (angl. REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC)[1]
e-storitev	Elektronska storitev
EKC	Enotni kontaktni center: služba za podporo uporabnikov (angl. Central contact point)
EU	Evropska unija (angl. European Union)
GTZ	Generične tehnološke zahteve (angl. Technical Guidelines for information solutions development)
NIO	Nacionalni interoperabilnostni okvir (angl. National Interoperability Framework)
SI-CAS	Centralni sistem za avtentikacijo, (angl. Central authentication system)
SI-CeP	Centralni sistem za e-pooblaščanje (angl.
SI-CeS	Centralni sistem za strežniško e-podpisovanje (angl. Central system for server-based e-signature)
SI-CeV	Centralni sistem za e-vročanje
SI-PASS	Sistem za avtentikacijo in e-podpis (angl. Authentication and e-Signature Service)
SI-PEPS	Centralni sistem za čezmejno avtentikacijo (angl. Central system for cross-border authentication)
SI-TRUST	Državni center za storitve zaupanja (angl. Trust Service Authority of Slovenia)
SI-TSA	Kvalificiran časovni žig
smsPASS	Mobilna identiteta (angl. Mobile based e-identity)

Pojmi v dokumentu:

- **Avtentikacija** je postopek preverjanje istovetnosti uporabnika, ali je uporabnik res ta, za katerega se predstavlja. Avtentikacija pomeni elektronski postopek, ki omogoča potrditev elektronske identifikacije fizične ali pravne osebe ali izvora in celovitosti podatkov v elektronski obliki (eIDAS).
- **Državni center za storitve zaupanja SI-TRUST** deluje v okviru Ministrstva za digitalno preobrazbo ter upravlja s korenskim izdajateljem SI-TRUST Root, izdajateljem kvalificiranih digitalnih potrdil SIGEN-CA, izdajateljem kvalificiranih digitalnih potrdil SIGOV-CA, izdajateljem kvalificiranih digitalnih potrdil SI-PASS-CA in izdajateljem kvalificiranih časovnih žigov SI-TSA. **Državni center storitev zaupanja SI-TRUST je skrbnik storitve za spletno prijavo in e-**

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

podpis SI-PASS in izdaja mobilno identiteto smsPASS oz. enkratno geslo, s katerim lahko oblikujete elektronski podpis dokumentov ter se prijavite v e-storitve, ki podpirajo smsPASS.

- **Elektronska identifikacija** pomeni postopek uporabe identifikacijskih podatkov osebe v elektronski obliki, ki enolično predstavljajo bodisi fizično ali pravno osebo bodisi fizično osebo, ki zastopa pravno osebo.
- **Ponudnik storitev** je organizacija, ki želi vključiti gradnike sistema SI-PASS v svoje spletne storitve.
- **Razvijalec,** je ekipa, ki za ponudnika storitve izvede integracijo storitve z gradniki sistema SI-PASS.
- **Integracija** je povezovanje posameznih enot, delov v večjo celoto, združevanje. Sistemska integracija je v inženirstvu opredeljena kot postopek združevanja sestavnih podsistemov v en sistem (združevanje podsistemov, ki sodelujejo tako, da sistem lahko zagotavlja splošno funkcionalnost), in zagotavljanje, da podsistemi delujejo skupaj kot sistem.
- **Skrbnik spletne storitve** je kontaktna oseba na strani ponudnika storitve;
- **Sredstvo elektronske identifikacije** - pomeni materialno in/ali nematerialno enoto, ki vsebuje identifikacijske podatke osebe in se uporablja za avtentikacijo pri spletnih storitvah (eIDAS)

1 UVOD

Smernice za uporabo in integracijo gradnikov sistema SI-PASS (v nadaljevanju: smernice) obravnavajo priporočila za vključitev gradnikov sistema SI-PASS v spletne storitve ponudnikov.

Sistem SI-PASS je enostaven in varen, zaupanja vreden centralni sistem za upravljanje:

- elektronskih identitet,
- elektronskega podpisovanje ter
- elektronskih pooblastil.

Sistem SI-PASS z uporabniškega vidika omogoča e-prijavo, e-podpis in e-pooblaščanje, z vidika ponudnikov in ustvarjalcev uporabniških storitev pa predstavlja nabor gradnikov, ki jih le ti lahko vključijo v svoja spletna mesta, spletne storitve za svoje uporabnike.

V okviru sistema SI-PASS so na voljo naslednji gradniki:

1. SI-CAS: centralni sistem za avtentikacijo,
    - SI-PEPS: centralni sistem za čezmejno avtentikacijo,
2. SI-CeS: centralni sistem za elektronsko podpisovanje na daljavo,
3. SI-CeP: centralni sistem za elektronsko pooblaščanje.

Zgornji gradniki in njihovo poimenovanje je namenjeno zgolj tehničnim razdelitvam funkcionalnosti sistema SI-PASS in so kot taki za uporabnika vidni le kot del funkcionalnosti sistema SI-PASS. Nazivi gradnikov se uporabljajo pri razvoju in integraciji v informacijske sisteme/storitve/aplikacije na spletu, zato vas nagovarjamo, da imen gradnikov ne uporabljate v drugih kontekstih, kot v razgovoru z razvijalci in skrbniki gradnikov.

Namen smernic je posredovati vodila vam, skrbnikom spletnih mest, spletnih rešitev in razvijalcem na podlagi katerih se boste lahko odločali, katere gradnike in na kakšen način boste uporabili pri izgradnji svojih sistemov, spletnih storitev.

Z uporabo gradnikov omogočite enovito uporabniško izkušnjo pri uporabi enakih funkcij pri spletnih storitvah, hrkati pa poenostavite procese razvoja in vzdrževanja funkcionalnosti, ki jih za vas v primeru uporabe gradnika izvedejo ustvarjalci in skrbniki gradnikov.

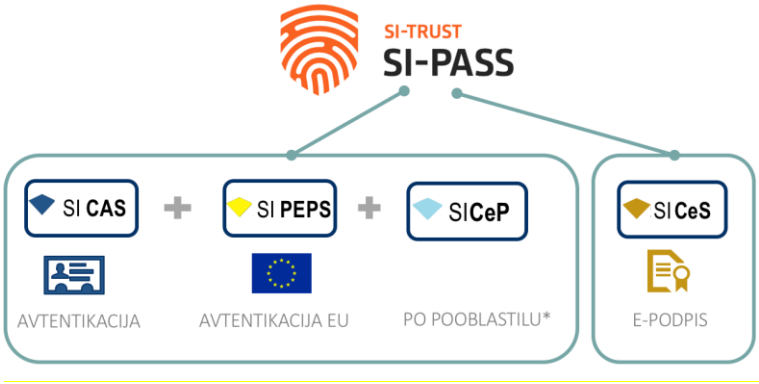
Natančna razlaga, namen in opis posameznega gradnika je v naslednjih poglavjih.

Glavne prednosti uporabe gradnikov sistem SI-PASS so predvsem: vse na enem mestu, posodobljeno, skladno z zakonskimi zahtevami, enovito.

Pričujoči dokument, Smernice za vpeljavo gradnikov SI-PASS vam podrobno razložijo korake in vas vodijo, s podrobnejšimi razlagami, skozi korake, ki so potrebni, da uspešno uporabite gradnike sistema SI-PASS v svoje spletne storitve. Pred odločitvijo o uporabi gradnikov sistema SI-PASS morate vedeti, kdo bodo vaši uporabniki, kako se bodo prijavljali v vašo spletno storitev in katere podatke o njih potrebujete.

2 SISTEM SI-PASS

Sistem SI-PASS sestavljajo različni gradniki, ki na enostaven način omogočajo podporo funkcionalnosti upravljanja e-identitet in e-podpisovanja.



Slika 1: Gradniki SI-PASS

* gradnik je še v razvoju

Sistem SI-PASS je centralni sistem za avtentikacijo in s tem enotna točka za preverjanje identitete različnih subjektov (državljanov, poslovnih subjektov, javnih uslužbencev in tujcev), ki povezuje e-identitete subjektov ter identifikacijske in druge podatke oz. atribute, shranjene pri različnih ponudnikih e-identitet in atributov ter storitev za e-podpisovanje.

Gradniki SI-PASS avtentikacije in pooblaščanja:

1. SI-CAS: centralni sistem za avtentikacijo domačih uporabnikov ter

   SI-PEPS: centralni sistem za avtentikacijo EU uporabnikov,
2. SI-CeP: centralni sistem za elektronsko pooblaščanje, ki je v zaključni fazi razvoja*.

Gradnik e-podpisa:

3. SI-CeS: centralni sistem za oddaljen e-podpis.

3 KORAKI VPELJAVE GRADNIKOV IN NJIHOVA UPORABA V SPLETNIH STORITVAH

V nadaljevanju je kratko zaporedje aktivnosti oziroma korakov, katerih izvedbo vam svetujemo, preden se odločite za uporabo gradnikov sistema SI-PASS.

1. Na portalu **NIO pridobite osnovne informacije o gradnikih SI-PASS:** dokumentacija SI-PASS (https://nio.gov.si/nio/asset/storitev+za+spletno+prijavo+in+epodpis+sipass)
2. Proučite **Smernice za vpeljavo gradnikov SI-PASS** ter izvedite **analiza potreb**, kjer v grobem identificirate:
    a. kdo so vaši uporabniki ter
    b. katere gradnike in na kakšen način boste uporabili.
3. Na portalu **NIO pridobite dokumentacijo** za posamezni gradnik,
4. Z razvojno ekipo preučite **izvedbo in načine integracije** gradnikov v spletne storitve
5. Detajlno določite kdo so **vaši uporabniki**
6. Določite katere **podatke o uporabnikih** potrebuje vaša spletna storitev
7. Izpolnite **vprašalnik** za posamezni gradnik, ki ga vključujete v svoje spletne storitve in ga posredujte na **Državni center za storitve zaupanja SI-TRUST**.
8. Z razvojno ekipo, v sodelovanju z **Državnim centrom storitev zaupanja SI-TRUST** svojo spletno storitev testno priklopite na **testni sistem SI-PASS**
9. V sodelovanju z **Državnim centrom za storitve zaupanja SI-TRUST** uskladite formalnosti in podpišete **Dogovor o uporabi sistema SI-PASS,**
10. V sodelovanju z **Državnim centrom za storitve zaupanja SI-TRUST** svojo spletno storitev preklopite na **produkcijski sistem SI-PASS**.

4 UPORABNIKI, NJIHOVI PODATKI IN NAČINI PRIJAVE

4.1 Določite, kdo so vaši uporabniki

V okviru koraka analize potreb se morate vprašati naslednja vprašanja:

- Kdo bodo uporabniki vaših storitev?
  - ✓ Državljani?
  - ✓ Podjetja?
  - ✓ Javni uslužbenci?
  - ✓ Tujci?
- Na kakšen način se bodo uporabniki prijavljali v vaša spletna mesta (kakšno raven zanesljivosti zahtevate)?
  - ✓ Z uporabniškimi imeni in gesli?
  - ✓ Z digitalnimi potrdili?
  - ✓ Preko sms-jev z uporabo telefonov?
- Ali za prijavo in delo uporabnikov z vašo spletno storitev potrebujete še dodatne vloge uporabnikov v sistemu? V kolikor ste iz javne uprave pa še, ali boste za ta namen uporabili gradnik Varnostne sheme, ki ga ravno tako ponuja Ministrstvo za javno upravo?

4.2 Določite podatke o uporabnikih

- Katere podatke potrebujete o uporabnikih vaših storitev kot rezultat avtentikacije (določitev identifikacijskih podatkov uporabnikov ter določitev obveznih podartkov):
  - ✓ Ime in priimek?
  - ✓ Davčno številko?
  - ✓ Naslov?
  - ✓ In drugi podatki, ki jih pridobite na podlagi prijave posameznika / uporabnika storitve in vpogleda v registre javne uprave.…
- Ali so zgornji podatki obvezni ali opcijski?
- Ali imate za pridobivanje in zbiranje teh podatkov pravno podlago?
- Ali spletne storitve vključujejo korak oddaje vlog in dokumentov, ki jih je potrebno podpisati? Boste za te namene uporabili gradnik oddaljenega e-podpisovanja?

Za spletno storitev morate določiti minimalen nabor identifikacijskih podatkov, atributov, ki morajo biti zanesljivi ali pridobljeni iz zunanjih virov in bodo za prijavo obvezni oziroma tiste, na podlagi katerih boste uporabnika vaše storitve prepoznali.

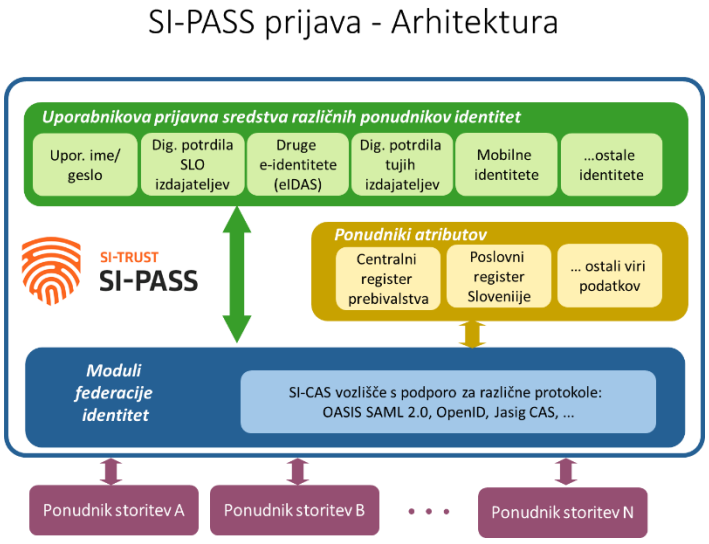
Za organe javne uprave je potrebno biti pozorni na pravno podlago, ki jo morate imeti, za pridobivanje in zbiranje osebnih podatkov, skladno z zakonodajo s področja varstva osebnih podatkov. Za vsak podatke v nabodu identifikacijskih podatkov morate določiti., ali je le-ta obvezen ali opcijski.

4.3 Prijava uporabnikov: SI-CaS, SI-PEPS, smsPASS

Uporaba centralne storitve za avtentikacijo uporabnikov SI-CAS je smiselna, ker gre za univerzalno zahtevo za vse storitve, ki zaradi **zagotavljanja varnosti** in **zaupanja** potrebujejo zanesljivo **ugotavljanje identitete posameznika**. S centralno podporo zagotovimo lažje upravljanje in podporo uporabi različnih elektronskih identifikatorjev različnih izdajateljev ter podporo različnim tehničnim rešitvam (npr. podporo za zanesljivo avtentikacijo preko mobilnih aparatov) in njihovemu razvoju.

Avtentikacija uporabnika je možna **z različnimi avtentikacijskimi** sredstvi **domačih** in **tujih** ponudnikov. Uporabniki se tako lahko avtenticirajo s prijavnimi sredstvi različnih **nivojev zaupanja**, od najnižjega nivoja (uporabniška imena in gesla, FB profil, …) do najvišjih nivojev (digitalno potrdilo, npr. na pametni kartici, mobilna identiteta smsPASS, osebna izkaznica), ki jih zagotavljajo različni ponudniki identitet.

Za prijavo v spletno storitev uporabite **gradnik SI-CAS za slovenske uporabnike, z domačimi sredstvi** za elektronsko identifikacijo in **gradnik SI-PEPS za dostop tujcev iz EU** z njihovimi **nacionalnimi sredstvi** za elektronsko identifikacijo.



Slika 2: Prijava uporabnikov v SI-PASS

4.3.1 Določitev ravni zanesljivosti

Preden začnete z razvojem storitve, določite ustrezno raven zanesljivosti, ki je za vašo spletno storitev zahtevana. Zahtevani nivo zaupanja je vedno določen s strani ponudnika spletne storitve, ki ga za potrebe avtentikacije uporabi gradnik SI-CAS.

Sredstva elektronske identifikacije so bolj ali manj odporna na zlorabe in spreminjanje identitet, zato je stopnja zanesljivosti v ugotovljeno e-identiteto uporabnika storitve v veliki meri odvisna od vrste uporabljene elektronske identifikacije. Prav tako imajo morebitne zlorabe in nepravilnosti pri ugotavljanju in preverjanju identitet različno resne posledice za različne storitve. Če kot ponudnik

storitev, želite preverjanje in potrjevanje e-identitete prenesti na gradnik SI-CAS, morate najprej določiti minimalno raven zanesljivosti sredstev elektronske identifikacije, ki je še sprejemljiva. Priporočljivo je, da izberete takšno raven zanesljivosti, ki najbolj ustreza vašim varnostnim zahtevam in morebitnim tveganjem. Nižja raven ni dopustna z varnostnega vidika, višja raven pa lahko naloži uporabnikom in vam - ponudniku storitev, dodatne zahteve in z njimi povezane stroške.

Ponudniki storitev morate za svojo spletno storitev izbrati najustreznejšo raven zanesljivosti in ustrezen način prijave, pri čemer pa si lahko pomagate s **Smernicami za izbiro ravni zanesljivosti SI-CAS** objavljenimi na portalu NIO: Smernice za izbiro ravni zanesljivosti SI-CAS[2]. Smernice za izbiro ravni zanesljivosti SI-CAS.

V smernicah so navodila za pripravo ocene tveganja, na podlagi katerega določite ustrezno raven zanesljivosti in način prijave. Določena raven je najnižja zahtevana raven, uporabniki pa se vedno lahko prijavijo tudi z višjimi.

Izbira ravni zanesljivosti predstavlja najnižji dovoljen nivo, uporabniki pa se seveda lahko vedno prijavi z identifikacijskimi sredstvi višjih ravni.

eIDAS določa naslednje ravni zanesljivosti:

- nizko [1],
- srednjo [2] in
- visoko [3]) raven za vsako sredstvo elektronske identifikacije, ki se izda v okviru posamezne sheme.

Dodatno pa je v okviru SI-PASS uvedena še zelo nizko raven zanesljivosti [0].

Raven zanesljivosti je odvisna od zahtev po primarnih in sekundarnih ukrepih, s katerimi se zmanjšajo tveganja.

Tabela v nadaljevanju prikazuje ravni zanesljivosti in načine prijave oziroma identifikacijska sredstva:

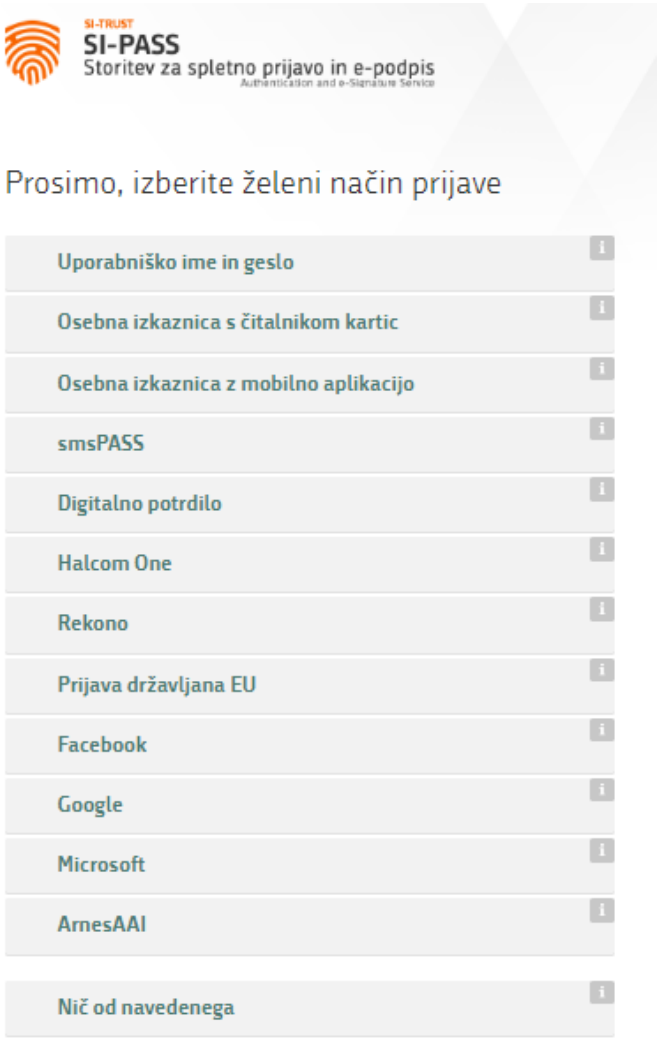
Raven zanesljivosti	Namen	Načini prijave
3 - visoka	**Zagotavlja višjo stopnjo zaupanja v izkazano ali zagotovljeno identiteto osebe kot sredstva elektronske identifikacije srednje ravni;** namen uporabljenih postopkov je preprečiti nevarnost zlorabe ali spreminjanja identitete	Sredstva visoke ravni zanesljivosti po uredbi eIDAS
		dvo-faktorska avtentikacija smsPASS
		prijava s kvalificiranim digitalnim potrdilom SIGOV-CA na pametni kartici
		prijava s kvalificiranim digitalnim potrdilom ponudnika storitev zaupanja na pametni kartici
		prijava s kvalificiranim digitalnim potrdilom ponudnika storitev zaupanja EU na pametni kartici

[2] Smernice za izbiro ravni zanesljivosti SI-CaS:
https://nio.gov.si/nio/asset/centralni+avtentikacijski+sistem+sicas

		prijava z elektronsko osebno izkaznico
2 - srednja	**Zagotavlja srednjo stopnjo zaupanja v izkazano ali zagotovljeno identiteto osebe;** Namen uporabljenih postopkov je znatno zmanjšati nevarnosti zlorabe ali spreminjanja identitete (*najnižji nivo, potreben za avtentikacijo za izvedbo elektronskega podpisa z gradnikom SI-CeS)	prijava z sredstvi višjih ravni
		sredstva srednje ravni zanesljivosti po uredbi eIDAS
		prijava s kvalificiranim digitalnim potrdilom SIGEN-CA
		prijava s kvalificiranim digitalnim potrdilom ponudniki storitev zaupanja
		prijava s kvalificiranim digitalnim potrdilom ponudnika storitev zaupanja EU
1 - nizka	**Zagotavlja omejeno stopnjo zaupanja v izkazano ali zagotovljeno identiteto osebe;** namen uporabljenih postopkov je zmanjšati nevarnost zlorabe ali spreminjanja identitete	prijava s sredstvi višjih ravni
		sredstva nizke zanesljivosti po uredbi eIDAS: Čezmejna prijava z uporabniškim imenom in geslom
		SI-PASS Poenostavljena prijava
0 - zelo nizka	**Zagotavlja minimalno stopnjo zanesljivosti v izkazano in nepreverjeno identiteto oseb;** namen uporabljenih postopkov je v manjši meri zmanjšati nevarnost zlorabe ali spreminjanja identitete	prijava s sredstvi višjih ravni
		prijava z geslom
		prijava s kvalificiranim digitalnim potrdilom poljubnega ponudnika storitve zaupanja
		Facebook
		Google
		Microsoft

Tabela 1: Ravni zanesljivosti in identifikacijska sredstva

Slika v nadaljevanju predstavlja načine prijave, ki jih SI-PASS zagotavlja ponudnikom storitve in njihovim uporabnikom s svojim gradnikom SI-CAS in se razlikujejo glede na priglasitev načinov prijave v določenem obdobju: SI-PASS načini prijave



Slika 3: Načini prijave SI-PASS[3]

4.3.2 Mobilna identiteta smsPASS oz. enkratno geslo smsPASS

V Sloveniji lahko državljani, poleg kvalificiranih digitalnih potrdil, za identifikacijo, uporabljajo tudi mehanizme mobilne identitete smsPASS. Mobilna identiteta smsPASS je način prijave v račun SI-PASS, ki s pomočjo enkratnega gesla, poslanega s kratkim sporočilom SMS, omogoča elektronsko zanesljivo identifikacijo uporabnika pri uporabi e-storitev in elektronsko podpisovanje dokumentov. Za uporabo smsPASS potrebujejo državljani mobilno telefonsko številko in telefon, ki sprejema kratka sporočila, ter napravo, povezano v splet (npr. računalnik, tablico, pametni telefon). Za uporabo smsPASSa mora imeti uporabnik SI-PASS račun.

Mobilno identiteto smsPASS lahko pridobijo osebe, ki imajo **slovensko davčno številko** in **EMŠO.**[4]

---

[3] Načini prijave SI-PASS: https://sicas.gov.si/bl/login?entityIDjson=7123QLa4DfGM8wFT47UFg8uLz%2Fvvz2EFFpAmlL256WoYPKv8ttbydw53Wzu8DXMrNSB%2BAK6OZWRHamNGFvLxj7Cnb0EfSLkEbZWx2csDsZU%3D

[4] Mobilna identiteta smsPASS: https://www.si-trust.gov.si/sl/si-pass/mobilna-identiteta/

4.3.3 Čezmejna prijava in skladnost z eIDAS: SI-PEPS

Pri načrtovanju prijave v vašo spletno storitev morate upoštevati tudi čezmejni vidik. V kolikor je za vašo spletno storitev potrebna čezmejna identifikacija, lahko za te namene uporabite gradnik SI-PEPS, ki predstavlja centralno vozlišče eIDAS, skladno z zahtevami.

Če nacionalno pravo ali upravna praksa za dostop do storitve, ki jo prek spleta zagotavlja organ javnega sektorja v eni državi članici, predpisuje elektronsko identifikacijo z uporabo sredstva elektronske identifikacije in avtentikacije, se sredstvo elektronske identifikacije, izdano v drugi državi članici, prizna v prvi državi članici za namene čezmejne avtentikacije za to spletno storitev, če so izpolnjeni naslednji pogoji:

a) sredstvo elektronske identifikacije je izdano v okviru sheme elektronske identifikacije;
b) raven zanesljivosti takšnega sredstva elektronske identifikacije ustreza ravni zanesljivosti, ki je enaka ali višja od ravni zanesljivosti, ki jo zahteva zadevni organ javnega sektorja pri dostopu do spletne storitve v prvi državi članici, pod pogojem, da raven zanesljivosti takšnega sredstva elektronske identifikacije ustreza srednji ali visoki ravni zanesljivosti;
c) zadevni organ javnega sektorja uporablja srednjo ali visoko raven zanesljivosti v zvezi z dostopom do te spletne storitve.[5]

Evropska infrastruktura eIDAS omogoča fizičnim in pravnim osebam, da uporabijo nacionalna sredstva za elektronsko identifikacijo za dostop do javnih in zasebnih e-storitev v drugih državah članicah EU.

4.3.3.1 Uporaba ustreznega jezika

Pri načrtovanju spletne prijave za tujce ali pri implementaciji spletne prijave v tujem jeziku morate upoštevati, da SI-PASS na podlagi parametrov podpira tudi angleški jezik. Za podrobnosti si poglejte tehnično dokumentacijo gradnika na portalu NIO.

4.3.4 Povezava z drugimi gradniki – Varnostna shema

V kolikor vaša spletna storitev za uporabo poleg identifikacijskih nivojev potrebuje dodatne podatke o vlogah uporabnikov, lahko uporabite skupni aplikacijski gradnik Varnostna shema. Varnostna shema je sistem za enotno upravljanje z uporabniki javne uprave in njihovimi pravicami, nadzor dostopa do aplikacij in njihovih funkcionalnosti.

Več o skupnem aplikacijskem gradniku Varnostna shema, si lahko preberete na portalu NIO: Skupni aplikacijski gradnik Varnostna shema.[6]

[5] Uredba eIDAS, Vzajemno priznavanje: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32014R0910&from=EN

[6] Skupni aplikacijski gradnik Varnostna shema: https://nio.gov.si/nio/asset/interoperabilnostna+komponenta+varnostna+shema-371

5 ELEKTRONSKI PODPIS: SI-CeS

Uporaba gradnika SI-CeS je smiselna, kadar v okviru svoje storitve potrebujete strežniško elektronsko podpisovanje s ključi imetnikov digitalnih potrdil, ki so varno shranjeni na centralnem sistemu. Povezava z gradnikom SI-CeS omogoča centralno e-podpisovanje v spletnih storitvah javne uprave za slovenske uporabnike in za tujce, ki želijo na daljavo opravljati spletne storitve v Sloveniji. Uporabnikom omogoča varen e-podpis brez nameščanja podpisnih komponent, kar olajša uporabo e-podpisa v različnih okoljih, tako stacionarnih kot tudi mobilnih.

Storitev elektronskega podpisovanja je prilagodljiva in podpira različne možnosti pri izvedbi e-podpisa: omogoča tvorbo e-podpisa v skladu z različnimi standardi oziroma formati (binarni, XML, PDF, CMS); podprto je oblikovanje e-podpisa različnih ravni (kvalificirani e-podpis, napredni e-podpis, overjen s kvalificiranim potrdilom, napredni e-podpis); uporabniku je na voljo več možnosti avtentikacije pri tvorbi e-podpisa glede na zahtevano raven e-podpisa in mehanizme avtentikacije, ki jih podpira centralni sistem za avtentikacijo SI-CAS. Storitev omogoča varen e-podpis brez nameščanja podpisnih komponent na strani uporabnika, kar podpira uporabo e-podpisa v vseh uporabniških okoljih, tako stacionarnih kot mobilnih.

Bistvena razlika, v primerjavi s splošno uveljavljenimi rešitvami za e-podpis je v načinu zagotavljanja, da je »zasebni ključ izključno pod nadzorom podpisnika«, saj je v tem primeru zasebni ključ imetnika varno shranjen v centralnem sistemu. Splošno uveljavljen način izpolnjevanja te zahteve temelji na varni hrambi in uporabi zasebnega ključa pri uporabniku, ključna funkcionalna zahteva storitve centralnega (strežniškega) e-podpisa pa je zagotavljati enak nivo zaupanja v elektronski podpis, kot ga zagotavljajo uveljavljene rešitve. Varnost zasebnih ključev imetnikov v centralnem sistemu je zagotovljena s tehničnimi mehanizmi, organizacijsko operativnimi ukrepi ter postopki upravljanja življenjskega cikla kriptografskih ključev in digitalnih potrdil. Za vsako aktivacijo zasebnega ključa imetnika se mora ta najprej ustrezno avtenticirati na sistemu SI-CAS, npr. s kvalificiranim digitalnim potrdilom, nato pa vpisati še geslo, s katerim je zaščiten njegov zasebni ključ.

SI-PASS e-podpis lahko uporabite na naslednje načine:

- e-podpis dokumentov / vlog skozi e-postopek,
- e-podpis dokumenta preko spletišča SI-PASS[7],
- preverjanje verodostojnosti e-podpisa (tudi iz tujine, pod določenimi pogoji)[8].

[7] Stran za izbiro načinov prijave za elektronski podpis: https://sicas.gov.si/CES-Sign/sign/index.htm

[8] Stran za izbiro načinov prijave za preverjanje podpisa: https://sicas.gov.si/CES-Sign/sign/validate.htm

6 DOKUMENTACIJA IN OPIS GRADNIKOV

Objave aktualnih informacij in dokumentov o modulih in gradnikih so objavljene na **portalu NIO**.[9]

6.1 SI-CAS

Naziv	Centralni sistem za avtentikacijo SI-CAS
Kratek opis	Centralni sistem za avtentikacijo SI-CAS (angl. *Slovenian Central Authentication System*) je namenjen integraciji funkcionalnosti ugotavljanja elektronske identitete v informacijske rešitve v okviru javnega sektorja. Ker gre za univerzalno zahtevo za vse storitve, ki zaradi zagotavljanja varnosti in zaupanja potrebujejo zanesljivo ugotavljanje identitete, je smotrna centralna storitev. Tako zagotovimo lažje upravljanje in podporo uporabi različnih elektronskih identifikatorjev različnih izdajateljev ter različnim tehničnim rešitvam (na primer podporo za uporabo digitalnih potrdil prek mobilnih aparatov) in njihovemu razvoju. Domači in tuji uporabniki se lahko identificirajo z e-identitetami različnih raven zaupanja, od najnižje ravni (uporabniška imena in gesla, FB-profil …) do najvišjih (e-identiteta na varnem mediju, na primer na pametni kartici), ki jih zagotavljajo različni ponudniki identitet. Zahtevano raven zaupanja določi ponudnik e-storitve, ki je za potrebe avtentikacije povezan s SI-CAS.
Status	Sistem je v uporabi. Na voljo je tudi testni sistem.
Uporaba	Za sisteme, ki potrebujejo avtentikacijo zunanjih (internetnih) uporabnikov **Opozorilo:** Od septembra 2018 je obvezna integracija na SI-CAS za vse sisteme javnega sektorja za izpolnjevanje zahtev 6. člena eIDAS)
Dokumentacija na portalu NIO:	PDF Navodila za priklop aplikacija na sistem SI-CAS (1060 KB)
	DOC Vprašalnik za zajem potreb novega uporabnika (52 KB)
	PDF Smernice za izbiro ravni zanesljivosti sredstva eID za dostop do e-storitev v JU (149 KB)
	PDF 10 korakov do skladnosti z eIDAS (83 KB)
	ZIP Pasica SI-CAS za ponudnike storitev (32 KB)

[9] Portalu NIO: https://nio.gov.si/nio/asset/storitev+za+spletno+prijavo+in+epodpis+sipass

	Modul razvojnega sistema pri ponudniku storitev (5 KB)
	Funkcionalne specifikacije in tehnična zasnova (814 KB)

6.2 SI-PEPS

Naziv	Centralni sistem za avtentikacijo čezmejnih uporabnikov SI-PEPS
Kratek opis	Centralni sistem za avtentikacijo čezmejnih uporabnikov SI-PEPS (angl. *Slovenian Central Authentication System*) predstavlja osrednje vozlišče eIDAS za Slovenijo, ki omogoča slovenskim uporabnikom enostaven dostop do javnih spletnih storitev v drugih državah članicah EU, tujcem iz EU pa dostop do slovenskih spletnih storitev z njihovimi nacionalnimi sredstvi za elektronsko identifikacijo.
Status	Sistem je v uporabi in je del sistema SI-CAS.
Uporaba	Za sisteme, ki potrebujejo avtentikacijo zunanjih (internetnih) uporabnikov. **Opozorilo:** Od septembra 2018 je obvezna integracija na SI-CAS za vse sisteme javnega sektorja za izpolnjevanje zahtev 6. člena eIDAS.
Povezava	

6.3 SI-CeS

Naziv	Centralni sistem za strežniško e-podpisovanje SI-CeS
Kratek opis	Centralni sistem za strežniško e-podpisovanje SI-CeS (angl. *Slovenian Central electronic Signiture*) omogoča oblikovanje elektronskega podpisa s ključi imetnikov digitalnih potrdil, ki so varno shranjeni v centralnem sistemu. Storitev je prilagodljiva in podpira različne možnosti pri izvedbi e-podpisa: omogoča tvorbo e-podpisa v skladu z različnimi standardi oziroma formati (binarni, XML, PDF, CMS); podprto je oblikovanje e-podpisa različnih ravni (kvalificirani e-podpis, napredni e-podpis, overjen s kvalificiranim potrdilom, napredni e-podpis); uporabniku je na voljo več možnosti avtentikacije pri tvorbi e-podpisa glede na zahtevano raven e-podpisa in mehanizme avtentikacije, ki jih podpira centralni sistem za avtentikacijo SI-CAS. Storitev omogoča varen e-podpis brez nameščanja podpisnih komponent na strani uporabnika, kar podpira uporabo e-podpisa v vseh uporabniških okoljih, tako stacionarnih kot mobilnih.
Status	Sistem je v uporabi (na voljo je tudi testni sistem).
Uporaba	Za sisteme, ki potrebujejo avtentikacijo zunanjih (internetnih) uporabnikov
Dokumentacija NIO:	Vprašalnik za zajem potreb novega uporabnika SI-CeS (49 KB)

	NAVODILA ZA PRIKLOP NA SISTEM SI-CeS v2.3 (1171 KB)
	Funkcionalne specifikacije (9868 KB) Brosura SI-CeS (534 KB)

Vključitev gradnika SI-CeS zahteva določene protokole in pravila, ki jih najdete v tehničnih specifikacijah, pri čemer razmisliti predvsem o smiselnosti uporabe gradnika v primeru občutljivih vsebin oziroma velikih dokumentov. V tem primeru lahko pride do določenih zamikov, ki v določenih primerih, v kolikor zahtevate oddajo in podpis dokumenta do določene ure, lahko predstavljajo oviro.

V kolikor so vaše spletne storitve vezane na točno določene čase oddaje vlog, obrazcev oziroma dokumentov, ki morajo biti podpisani, njihovi uporabniki pa v večini primerov oddajajo le te v zadnjem hipu, je potrebno razmisliti o načinu vključitve gradnika za elektronsko podpisovanje, hkrati pa opozoriti uporabnike, da čas podpisa lahko traja nekaj časa.

6.4 SI-CEP

Naziv	Centralni sistem za elektronsko pooblaščanje SI-CEP
Kratek opis	Centralni sistem za elektronsko pooblaščanje SI-CEP (angl. *Slovenian Central electronic Mandate*) je namenjen pripravi elektronskih pooblastil za storitve javne uprave in omogoča oddajo, preklic, zamrznitev in uporabo elektronskih pooblastil med pooblastitelji in pooblaščenci.
Status	Sistem je v zaključni fazi razvoja, predvidoma bo na voljo tekom leta 2024.
Uporaba	
Povezava	

7 PROUČITEV IZVEDBE IN NAČINOV INTEGRACIJE GRADNIKOV

V tehnični dokumentaciji posameznega gradnika so zapisane lastnosti gradnika in zahteve ter načini integracije posameznega gradnika. Z razvijalcem, ki ste ali pa ga boste izbrali, za vključitev določenega gradnika v svojo spletno storitev, skupaj preglejte dokumentacijo in zahteve, ter pogoje vključitve gradnika.

7.1 Vprašalniki za posamezni gradnik

Pred vključitvijo vaše spletne storitve v testni sistem sistema SI-PASS, morate izpolniti vprašalnik za zajem potreb za ustrezen gradnik, ki ga želite vključiti.

V vprašalniku za zajem potreb morate določiti najmanj:

- Opis spletne storitve
- Uporabnike: število, vrsta uporabnikov in institucije
- Predvideni načini uporabe
- Zahtevana ravne zanesljivosti
- Identifikacijski podatki uporabnikov
- Predvideni rok za integracijo
- Kontaktne osebe.

V zvezi z določitvijo oziroma analizo potreb avtentikacije SI-CaS izpolnite **vprašalnik za zajem potreb novega uporabnika** na portalu NIO: Vprašalnik za zajem potreb novega uporabnika [10].

Pred odločitvijo in vpeljavo gradnika za elektronsko podpisovanje SI-CeS pa odgovorite na vprašalnik za zajem potreb novega uporabnika SI-CeS, objavljenega na portalu NIO: Vprašalnik za zajem potreb novega uporabnika SI-CeS[11].

V kolikor imete kakršnekoli nejasnosti, se obrnite na Državni center za storitve zaupanja.

7.2 Testna namestitev

Testno okolje za uporabo sistema SI-PASS je popolnoma ločeno okolje, ki je povezano s testnimi okolji virov, kar pomeni, da podatki, ki jih dobite v fazi testiranja niso realni.

Za namestitev v testno okolje morate izpolniti vprašalnik, ki je objavljen na portalu NIO, za vsak gradnik posebej. Za integracijo SI-CAS je potrebna še metadata datoteka, za SI-CeS pa prijava s potrdilom, ali podatki o potrdilu, da se dodelijo pravice.

Pri vzpostavitvi testnega okolja in uporabi testnega sistema SI-PASS se morate zavedati, da je testno okolje, zaradi varstva osebnih podatkov, povezano s testnimi podatki Centralnega Registra Prebivalcev (CRP). Osebni podatki so v testnem okolju spremenjeni, zato morate poskrbeti, da SI-

[10] Vprašalnik za zajem potreb novega uporabnika: https://nio.gov.si/nio/asset/centralni+avtentikacijski+sistem+sicas

[11] Vprašalnik za zajem potreb novega uporabnika SI-CeS: https://nio.gov.si/nio/asset/centralni+sistem+za+streznisko+epodpisovanje+sices

TRUST potrdila, ki so najverjetneje produkcijska, registrirate za uporabo v testnem okolju (za davčno številko produkcijskega potrdila boste prejeli neko drugo - izmišljeno ime in priimek), kar pa sicer ni neposredno odvisno od SI-PASS.

Za potrebe testiranja sistema SI-PASS morate ustvariti testne SI- PASS račune. V primeru testiranja s SIGOV-CA, SIGEN-CA potrdili ali nove elektronske osebne izkaznice je potrebno oddati zahtevek za vpis v testno prevajalno tabelo.

8 DOGOVOR O UPORABI SISTEMA SI-PASS

Pred prehodom na produkcijsko uporabo gradnikov sistema SI-PASS morate z Državnim centrom storitev zaupanja SI-TRUST podpisati dogovor o uporabi sistema SI-PASS, v obliki pogodbe, kjer dogovorite predmet (vsebino), razmerja in odgovornosti.

Ponudnik storitve se z dogovorom zaveže, da bo upošteval vse pogoje in navodila objavljena na portalu NIO ter spremljal vsa obvestila o varnostnih priporočilih in jih upošteval pri uporabi sistema.

8.1 Prehod v produkcijo in zagotavljanje delovanja

Pred prehodom v produkcijo morate preveriti izpolnjevanje pogojev, ki so priloga dogovora in vključujejo podatke o kriptografskih ključih in potrdilih, metapodatkih, atributov. Preveriti morate, ali ste upoštevali zahtevane funkcionalnosti vključitve gradnikov ter varnostne zahteve in pravočasno obveščati skrbnika sistema o spremembah in drugih dejstvih, ki bi vplivala na vključevanje gradnikov.

9 PRIPOROČILA ZA UMESTITEV GRADNIKOV SI-PASS IN NJIHOVIH VIZUALNIH DELOV V SPLETNE STORITVE

Pri vpeljavi gradnikov SI-PASS v vaše spletne storitve je potrebno upoštevati nekaj pravil njihove vpeljave. Poleg sledenja navodil za priklop morate slediti tudi **Navodilom za vključitev grafičnih elementov gradnikov SI-PASS**, ki je priloga tega dokumenta. Želimo si namreč, da imajo vse strani, kjer so vključeni gradniki enotne grafične elemente SI-PASS, ki uporabniku na enostaven način sporočajo, kje so in kaj uporabljajo.

Dobra uporabniška izkušnja in sprejemljivost s strani uporabnikov sta pomembna dejavnika uspešnosti uvajanja varnostnih storitev v praksi. K boljši uporabniški izkušnji in sprejemljivosti prispevajo popolnost in jasnost posredovanih informacij, na primer varnostnih opozoril in obvestil v primeru napak, jasnost predstavitve in uporaba uveljavljenih grafičnih elementov, smiselnost in učinkovitost posameznih korakov pri uporabi, prilagodljivost predstavitve glede na vrsto naprave, s katero uporabnik dostopa do storitve, in dostopnost za uporabnike s funkcijskimi omejitvami (deprivilegirane uporabnike). V nadaljevanju so podana osnovna priporočila za povečanje uporabnosti in dostopnosti storitev, povezanih s sistemom SI-PASS.

Pri vključitvi gradnikov v spletne storitve morate, v primeru, da ste organ javne uprave, slediti zahtevam Uredbe o celostni grafični podobi Vlade Republike Slovenije in drugih organov državne uprave in pravil umeščanja enotnih grafičnih elementov na spletnih mestih organov državne uprave, kjer bodite še posebno pozorni na elemente v povezavi s sistemom SI-PASS.

9.1 Varnostna opozorila

Varnostna opozorila in opozorila v primeru napak morajo biti natančna in lahko razumljiva. Opozorila naj vsebujejo tudi kratka navodila, kaj je treba storiti drugače, da ne bi prišlo do ponovne napake, na primer, če uporabnik pri prijavi izbere napačno digitalno potrdilo.

Uporabniku se ne sme prikazati obvestilo, da digitalno potrdilo spletnega strežnika ponudnika storitve ni veljavno ali zaupanja vredno. Na spletni strani ponudnika mora biti mogoče razbrati, katero korensko potrdilo si mora uporabnik namestiti, da bo digitalno potrdilo spletnega strežnika zaupanja vredno.

9.2 Časovne omejitve

Uporabnik naj ima dovolj časa za izvedbo posameznih aktivnosti. Kadar je mogoče, naj bodo časovne omejitve prilagodljive.

10 ZADOVOLJSTVO UPORABNIKOV

Z namenom nenehnega izboljševanja storitev vas vabimo, da zbirate zadovoljstvo uporabnikov tudi v zvezi z uporabo gradnikov in nas o tem obveščate na naslov si-pass@gov.si.

Stik:

Ministrstvo za digitalno preobrazbo

Direktorat za razvoj digitalnih rešitev in podatkovno ekonomijo

Državni center za storitve zaupanja SI-TRUST

gp.mju@gov.si

11 PRILOGE

11.1 Priloga 1: Sistem SI-PASS: Splošni pogoji uporabe za organe in druge pravne osebe

11.2 Priloga 2: Navodila za vključitev grafičnih elementov gradnikov SI-PASS