REPUBLIKA SLOVENIJA

MINISTRSTVO ZA PRAVOSODJE IN JAVNO UPRAVO

Tržaška cesta 21, 1000 Ljubljana

Naložba v vašo prihodnost
OPERACIJO DELNO FINANCIRA EVROPSKA UNIJA
Evropski socialni sklad

Slovenia Business Point

Centralni avtentikacijski sistem SI-CAS

Naloga:

Priprava funkcionalnih specifikacij in tehnične zasnove centralnega avtentikacijskega sistema (CAS).

STANJE DOKUMENTA

Namen:	Funkcionalne specifikacije in tehnična zasnova centralnega avtentikacijskega sistema (SI-CAS)
Vsebina:	Vsebina dokumenta je vidna iz kazala.
Oznaka:	EKT2-CAS-FS
Status:	Končna verzija za potrjevanje
Verzija:	1.0, glej »Zgodovina sprememb«
Datum verzije:	26. november 2012
Stanje:	Dokument ni lektoriran.
Lastnik	Ministrstvo za pravosodje in javno upravo
Avtorji:	Rudi Ponikvar OSI d.o.o., Delovna skupina EKT2-CAS

ZGODOVINA SPREMEMB

Verzija	Datum	Razlog za spremembe	Spremenil
1.0	26.11.2012	Končna verzija za potrjevanje	Rudi Ponikvar OSI d.o.o., Delovna skupina EKT2-CAS
1.1	10.1.2013	Raziskava trga	Delovna skupina EKT2-CAS

KAZALO

1 Uvod

Ministrstvo za pravosodje in javno upravo (v nadaljevanju *MPJU*) vzpostavlja Centralni avtentikacijski sistem za potrebe javne uprave (v nadaljevanju *SI-CAS*), ki bo omogočil poenoteno preverjanje identitete in opcijsko enkratno prijavo uporabnikov (angl. Single Sign-On, SSO).

SI-CAS bo enotna točka za preverjanje identitet različnih subjektov (državljanov, poslovnih subjektov, javnih uslužbencev) po? konceptu federacije identitet, ki povezuje elektronske identitete subjektov in identifikacijske podatke (atribute), shranjene pri različnih izdajateljih e-identitet (ponudnikih identitet) in atributov.

1.1 Namen in cilji

Vzpostavitev SI-CAS je namenjena za potrebe integracije funkcionalnosti ugotavljanja elektronske identitete v informacijske rešitve v okviru javnega sektorja. Centralna storitev je smiselna, ker gre za univerzalno zahtevo za vse storitve, ki zaradi zagotavljanja varnosti in zaupanja potrebujejo zanesljivo ugotavljanje identitete. S centralno podporo zagotovimo lažje upravljanje in podporo uporabi različnih elektronskih identifikatorjev različnih izdajateljev ter podporo različnim tehničnim rešitvam (npr. podporo za uporabo digitalnih potrdil preko mobilnih aparatov) in njihovemu razvoju.

Zaradi zahtev po delovanju notranjega trga EU je potrebno zagotoviti, da bo centralna storitev podpirala tudi ugotavljanje istovetnosti tujih subjektov, ki bodo avtentikacijo opravile z uporabo elektronskih identifikatorjev iz drugih držav. V ta namen bo SI-CAS upošteval rezultate drugih aktivnosti na tem področju, od pravnih in strateških usmeritev do konkretnih implementacij, ki so bile razvite v okviru projektov, predvsem EU pilotnega projekta velikih razsežnosti za čezmejno avtentikacijo STORK (več o tem na spletni strani www.eid-stork.eu/).

Domači in tuji uporabniki se bodo lahko identificirali z e-identitetami različnih nivojev zaupanja, od najnižjega nivoja (uporabniška imena in gesla, FB profil[1], …) do najvišjih nivojev (e-identiteta na varnem mediju, npr. na pametni kartici)), ki jih bodo zagotovili različni ponudniki identitet . Zahtevani nivo zaupanja bo določen s strani ponudnika e-storitve, ki bo za potrebe avtentikacije povezan na SI-CAS.

[1] *Facebook* profil

1.2 Podlaga za vzpostavitev SI-CAS

Izdelava SI-CAS je predvidena tudi v strateških dokumentih, ki usmerjajo razvoj e-uprave na nacionalnem nivoju:

- Strategija razvoja elektronskega poslovanja ter izmenjave podatkov iz uradnih evidenc, 2009 ,
- Akcijski načrt e-poslovanja v javni upravi do 2015, 2010 (v nadaljevanju *AN SREP*).

Eden izmed ključnih ciljev je tudi razvoj skupnih in integriranih storitev med vsebinskimi področji in nivoji uprave, kar pomeni razvoj e-uprave s pomočjo centralnih horizontalnih podpornih funkcij in storitev. Tak način naj bi omogočil lažji razvoj novih elektronskih storitev, čas za njihovo implementacijo bi se krajšal, stroški bi bili nižji, obenem pa bi bila zagotovljena večja interoperabilnost med institucijami in med rešitvami. Eno izmed pomembnih področij, ki jih je smiselno zagotavljati skozi skupne rešitve, je prav področje identifikacije in avtentikacije. SI-CAS je zato pomemben ukrep, ki bo pripomogel k ciljem, zadanim z navedenimi strateškimi dokumenti in njihovimi cilji.

Skladno s priporočili OECD (Organizacija za gospodarsko sodelovanje in razvoj) in smernicami standardizacijskega telesa ETSI (European Telecommunications Standards Institute) bo za delovanje SI-CAS izdelana tudi enovita politika za avtentikacijo.

Pri vzpostavitvi sistema SI-CAS bo potrebno upoštevati tudi morebitne spremembe zakonodaje, ki ureja to področje na nacionalni kot tudi na ravni EU. V okviru EU je tako že v pripravi Uredba o e-identifikaciji in skrbniških storitvah (v nadaljevanju *eIDAS*), ki bo dodatno urejala tudi področje identifikacije oz. avtentikacije uporabnikov.

1.3 SI-CAS in projekt EKT2

Direktiva 2006/123/ES o storitvah na notranjem trgu (v nadaljevanju Storitvena direktiva) predstavlja velik korak naprej pri zagotavljanju svobode ustanavljanja podjetij in čezmejnega opravljanja storitev. Ena pomembnih zahtev direktive se nanaša na vzpostavitev enotne kontaktne točke (v nadaljevanju EKT), ki jo morajo izpolniti vse države članice, tako za domače kot tudi za tuje ponudnike, za opravljanje dejavnosti oziroma storitev. Preko EKT bodo državljani EU v posamezni državi članici dobili vse informacije, ki jih potrebujejo za vstop na njen trg (npr. informacija o postopku pridobitve obrtnega dovoljenja, informacija o postopku pridobitve turistične licence ipd.) in imeli tudi možnost, da preko te točke pridobijo dovoljenje na daljavo (preko spleta). Zahteva za čezmejno opravljanje storitev v praksi predstavlja celo vrsto interoperabilnostnih izzivov, ki jih države članice skupaj z Evropsko komisijo rešujejo v okviru različnih aktivnosti, njihova podlaga pa je zajeta v različnih strateških dokumentih za razvoj e-uprave na ravni EU.

Projekt EKT 2 bo realiziral elektronsko podporo in preko EKT omogočil pridobivanje dovoljenj na daljavo. Ker je potrebno v okviru projekta zagotoviti visoko stopnjo zrelosti e-storitev in

integriranosti le-teh (zajele bodo številne institucije bodisi zaradi pridobivanja dovoljen, bodisi zaradi pridobivanja dokazil oz. podatkov) ter zagotoviti tudi čezmejnost, je eden izmed glavnih izzivov projekta zagotavljanje interoperabilnosti, tako nacionalne kot tudi čezmejne. Prav zato je eden izmed glavnih ciljev projekta je tudi vzpostavitev horizontalnih/centralnih funkcij skladno z AN SREP oz. izgradnja različnih modulov in integracija teh modulov v povezljiv in odprt sistem z integracijo na vse obstoječe sisteme, ki bistveno prispevajo k funkcionalnosti novega sistema in predstavljajo ciljno dodano vrednost. Tako se bodo v okviru EKT 2 uvedel poenoten sistem e-dokumentov, rešitve za katalog storitev, tako za urejenost in lažjo dostopnost do postopkov posameznih institucij kot tudi za dostop do e-storitev (npr. e-vročanje itd.), register postopkov, sistem za kratkoročno hrambo dokumentarnega gradiva, sistem sindikacije za avtomatski prenos vsebine oz. opisov od pristojnih institucij do EKT ter nenazadnje vzpostavitev centralne storitve za avtentikacijo (SI-CAS), ki je tudi predmet obravnavanega dokumenta.

2 SI-CAS koncepti in pojmi

Osnovni namen SI-CAS je integracija funkcionalnosti ugotavljanja elektronske identitete uporabnikov v informacijske rešitve v okviru javnega sektorja. Vzpostavljen bo kot centralna storitev za preverjanje identitet v spletnih storitvah. Identifikacija bo možna z različnimi identitetami domačih in tujih uporabnikov oziroma domačih in tujih ponudnikov identitet.

SI-CAS evidenca uporabnikov razen ustrezno (npr. z zgostitveno funkcijo) zaščitenih osnovnih identifikatorjev ne bo vsebovala identifikacijskih podatkov uporabnikov, temveč informacije, pri katerem ponudniku identitet ima posamezen uporabnik registrirano svojo elektronsko identiteto in pri katerem ponudniku atributov se nahajajo dodatni identifikacijski podatki oziroma atributi.

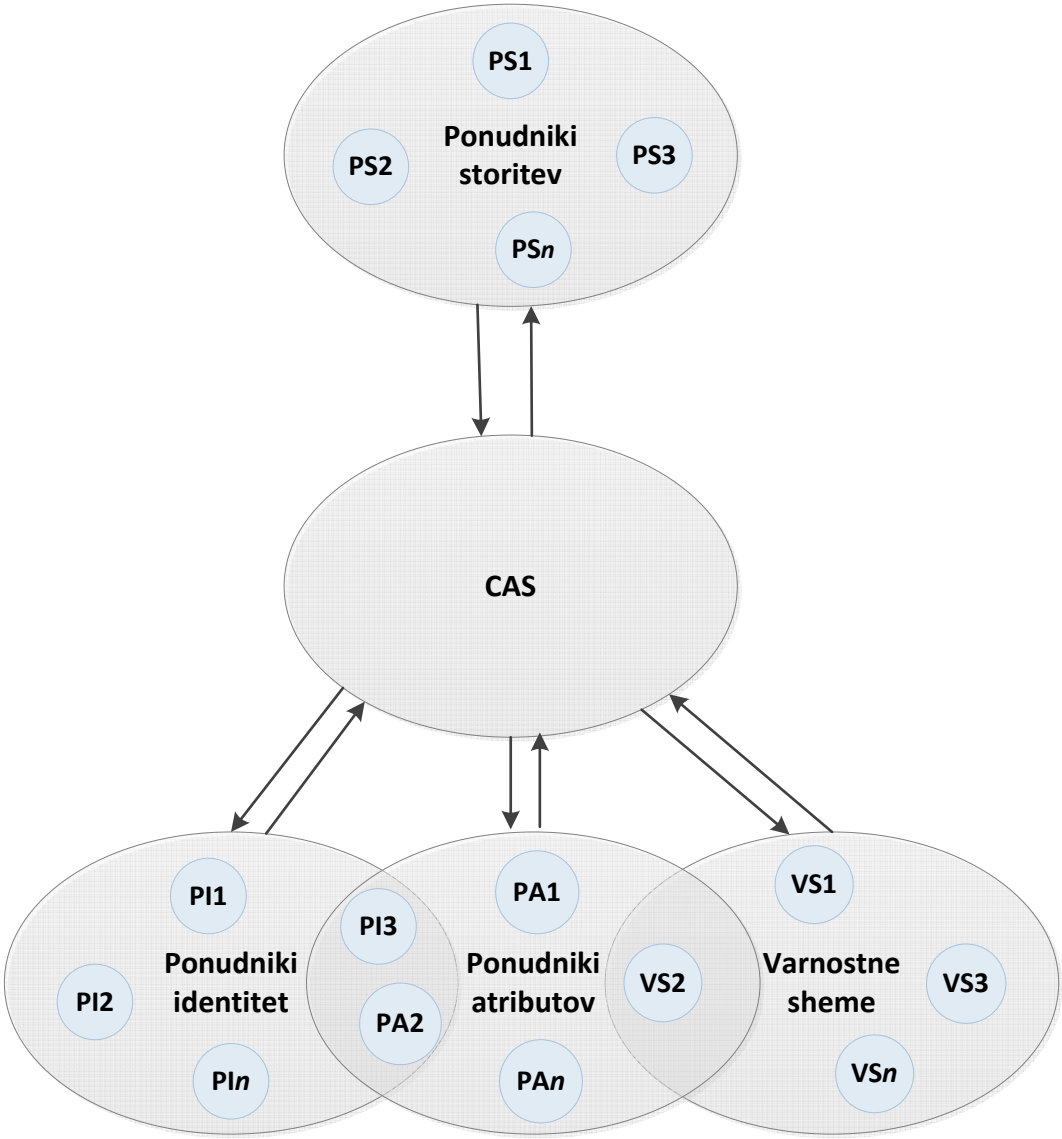
Ponudniki storitev se ne bodo povezovali z vsakim ponudnikom identitet in ponudnikom atributov posebej, temveč le s SI-CAS. SI-CAS bo v procesu deloval kot zaupanja vreden posrednik. Na zahtevo ponudnika storitev bo preveril identiteto uporabnika pri ustreznem ponudniku identitet in po potrebi pridobil dodatne identifikacijske atribute pri ponudniku identitet. SI-CAS bo imel v ta namen vzpostavljeno direktno zaupanje s ponudniki storitev, ponudniki identitet in ponudniki atributov. Zaupanje bo vzpostavljeno na tehnološkem in formalnem nivoju.

V nadaljevanju so opisani sledeči ključni pojmi in koncepti, ki so osnova za vzpostavitev SI-CAS:

- SI-CAS jedro (Centralni avtentikacijski sistem - CAS, angl. Federated Identity Provider).
- Identiteta, Identifikator, Identifikacijski mehanizem.
- Ponudnik identitet (PI,angl. Identity Provider).
- Ponudnik atributov(PA, angl. Attribute Provider).
- Ponudnik storitev (PS, angl. Service Provider).
- Varnostna shema(VS, angl. AuthorizationProvider).

- Enkratna prijava (angl. Single Sign-On, SSO)
- Varnostne izjave (angl. Security Assertions).
- Registracija identitete, povezovanje identitet.
- Dodatne centralizirane storitve za podporo elektronskega poslovanja (niso del SI-CAS):
  - centralna validacija digitalnih potrdil,
  - centralna validacija digitalnih podpisov,
  - strežniški podpis končnega uporabnika.

Sledeča shema prikazuje model SI-CAS sistema kot centralnega posrednika med ponudniki storitev (PS), ponudniki identitet (PI), ponudniki atributov (PA) in varnostno shemo (VS).



2.1 SI-CAS jedro – Centralni avtentikacijski sistem

Glavne funkcije SI-CAS jedra so zagotavljanje zaupanja med ponudniki storitev in različnimi ponudniki identitet, kar obsega:

- vzpostavitev mehanizmov in protokolov za sprejemanje zahtevkov za preverjanje identitet od ponudnikov storitev,
- preverjanje identitet pri registriranih ponudnikih identitet,
- pridobitev podatkov o avtenticiranih subjektih,
- filtriranje podatkov glede na ponudnika storitev (katere podatke se mu lahko posreduje),
- pridobitev dodatnih podatkov preko ponudnikov atributov,
- posredovanje identifikacijskih podatkov ponudniku storitev.

2.2 Identiteta, identifikator, identifikacijski mehanizem

2.2.1 Identiteta

Identiteto predstavlja nabor podatkov, ki enolično opisuje določen subjekt. Nabor identifikacijskih podatkov obsega podatke, na osnovi katerih lahko enolično prepoznamo subjekt ter ga povežemo s podatki ali funkcijo v okviru aplikacije ponudnika storitve. Nabor podatkov obsega enolični identifikator (angl. Unique Identifier, UID) na nivoju ponudnika identitet ter dodatne osebne in/ali javne podatke (atribute), ki opisujejo subjekt.

2.2.2 Identifikator

Identifikator je oznaka, ki jo ponudnik identitet dodeli subjektu. Na nivoju ponudnika identitet se uporablja za povezovanje subjekta in pripadajočih identifikacijskih podatkov. Na nivoju ponudnika storitev se identifikator uporablja za povezovanje subjekta z njegovimi podatki in/ali funkcijami na nivoju posamezne aplikacije.

Identifikator mora biti enoličen na nivoju ponudnika identitet in ponudnika storitev. V primeru povezovanja identitet različnih ponudnikov identitet in uporabi pri različnih ponudnikih storitev je potrebno oziroma zaželeno, da je identifikator enoličen tudi na nivoju vseh ponudnikov identitet (angl. Globally Unique Identifier, GUID).

2.2.3 Identifikacijski mehanizem

Ponudniki identitet lahko uporabljajo različne identifikacijske mehanizme za avtentikacijo uporabnikov, kot so na primer:

- repozitorij uporabniških imen in gesel,
- X.509 digitalna potrdila izdana na pametni kartici,
- X.509 digitalna potrdila + geslo,
- RADIUS,

- LDAP imenik,
- Kerberos.

2.3 Ponudnik identitet

Ponudnik identitet je storitev, ki upravlja identitete uporabnikov, izvaja preverjanje identitet (avtentikacijo) ter po izvedeni avtentikaciji posreduje podatke o identiteti uporabnika ponudniku storitev. Ponudnik identitet lahko uporablja enega ali več identifikacijskih mehanizmov, kot so uporabniška imena in gesla, digitalna potrdila, LDAP imenik, RADIUS, Kerberos ipd. Ponudnik identitet je lahko hkrati tudi ponudnik atributov.

Nivoji zaupanja v identiteto uporabnika se opredelijo z nivoji zaupanja ali kot profili, ki bodo določeni v SI-CAS politiki za avtentikacijo. Nivo zaupanja oziroma profil odraža zaupanje v mehanizem preverjanja identitete ob registraciji in uporabljen identifikacijski mehanizem.

2.4 Ponudnik atributov

Ponudnik atributov je ponudnik storitev, ki upravlja nabor podatkov o subjektih. Ponudnik atributov je lahko samostojna storitev ali pa je vzpostavljena v okviru ponudnika identitet.

2.5 Ponudnik storitev

Ponudnik storitev v okviru svojih storitev zagotavlja eno ali več aplikacij za končne uporabnike. Ponudnik storitev uporablja CAS za preverjanje identitete uporabnikov ter pridobitev identifikacijskih in drugih podatkov. Ponudnik storitev na osnovi pridobljene identitete in podatkov (atributov) poveže uporabnika z internimi podatki in/ali pooblastili ter mu na osnovi tega omogoči izvajati določene storitve.

2.6 Varnostna shema

Obstoječa rešitev Varnostne sheme se bo v sklopu SI-CAS predvidoma uporabila kot ponudnik atributov in sicer na dva načina:

- atributi v Varnostni shemi so lahko varnostni nivoji glede na identifikacijski mehanizem in drugi atributi, potrebni za osnovne funkcionalnosti SI-CAS,
- atributi v Varnostni shemi so lahko vezani na pooblastila posameznega subjekta znotraj določene aplikacije ponudnika storitev, kar predstavlja sedanji način uporabe Varnostne sheme.

Atributi v Varnostni shemi so lahko splošni (privzeti na nivoju SI-CAS) ali pa specifični za posameznega ponudnika storitev oziroma aplikacijo.

Opis implementacije obstoječe Varnostne sheme je podan v Prilogi 1.

2.7 Enkratna prijava

Enkratna prijava omogoča, da uporabnik po prijavi dostopa do različnih storitev, ne da bi se mu bil potrebno prijavljati v vsako storitev posebej.

2.8 Varnostne izjave

Varnostne izjave so mehanizem, preko katerega:

- ponudnik identitet potrdi, da je preveril pristnost uporabnika,
- ponudnik identitet jamči za posredovano identiteto uporabnika,
- ponudnik identitet ali ponudnik atributov jamči za posredovane atribute.

Varnostne izjave lahko vsebujejo informacije:

- o identiteti uporabnika (edinstveni identifikator, informacijo o ponudniku identitete, …),
- o dodatnih atributih (npr. naslov elektronske pošte, datum rojstva, …),
- ali ima uporabnik pravico dostopa do storitve, podatka, akcije, …

Integriteta varnostnih izjav je zagotovljena z XML digitalnim podpisom. Posamezni atributi, vsebovani v varnostni izjavi, so lahko tudi šifrirani, v primeru, da je potrebno zaradi narave podatkov zagotoviti njihovo zaupnost.

2.9 Dodatne centralizirane storitve za podporo elektronskega poslovanja (niso del osnovnega SI-CAS)

Dodatne centralizirane storitve za podporo elektronskega poslovanja lahko obsegajo npr.:

- centralno validacijo digitalnih potrdil kot samostojno storitev,
- centralno validacijo digitalnih podpisov,
- strežniški podpis v imenu končnega uporabnika.

Dodana vrednost navedenih centraliziranih storitev je:

- poenoteno preverjanje zaupanja v digitalna potrdila,
- storitve validacije digitalnih potrdil lahko uporablja tudi SI-CAS za preverjanje potrdil in pridobitev identifikacijskih podatkov (atributov) iz digitalni potrdil,
- poenotenje oblik digitalnega podpisa,
- poenostavi se implementacija aplikacij, ker teh storitev ni potrebno implementirati na nivoju posamezne aplikacije,
- strežniški podpis v imenu končnega uporabnika praktično odpravlja potrebo razvoja in nameščanja podpisne komponente na strani uporabnika.

3 Izhodišča za integracijo obstoječih rešitev s SI-CAS

Sistem SI-CAS bo predvidoma podpiral tako nove storitve, kot je npr. EKT, kakor tudi obstoječe storitve. Obstoječe storitve imajo praviloma že vzpostavljene rešitve za avtentikacijo in avtorizacijo uporabnikov ter po potrebi tudi za pridobitev atributov. V večini primerov tako ponudnik storitve v okviru posamezne rešitve zagotovi implementacijo oziroma integracijo vseh ostalih komponent, to je ponudnika identitet, ponudnika atributov in Varnostne sheme.

V okviru pregleda možnosti prehoda obstoječih rešitev na SI-CAS so bile za posamezne storitve, ki so potencialni uporabniki sistema SI-CAS, pridobljene naslednje informacije:

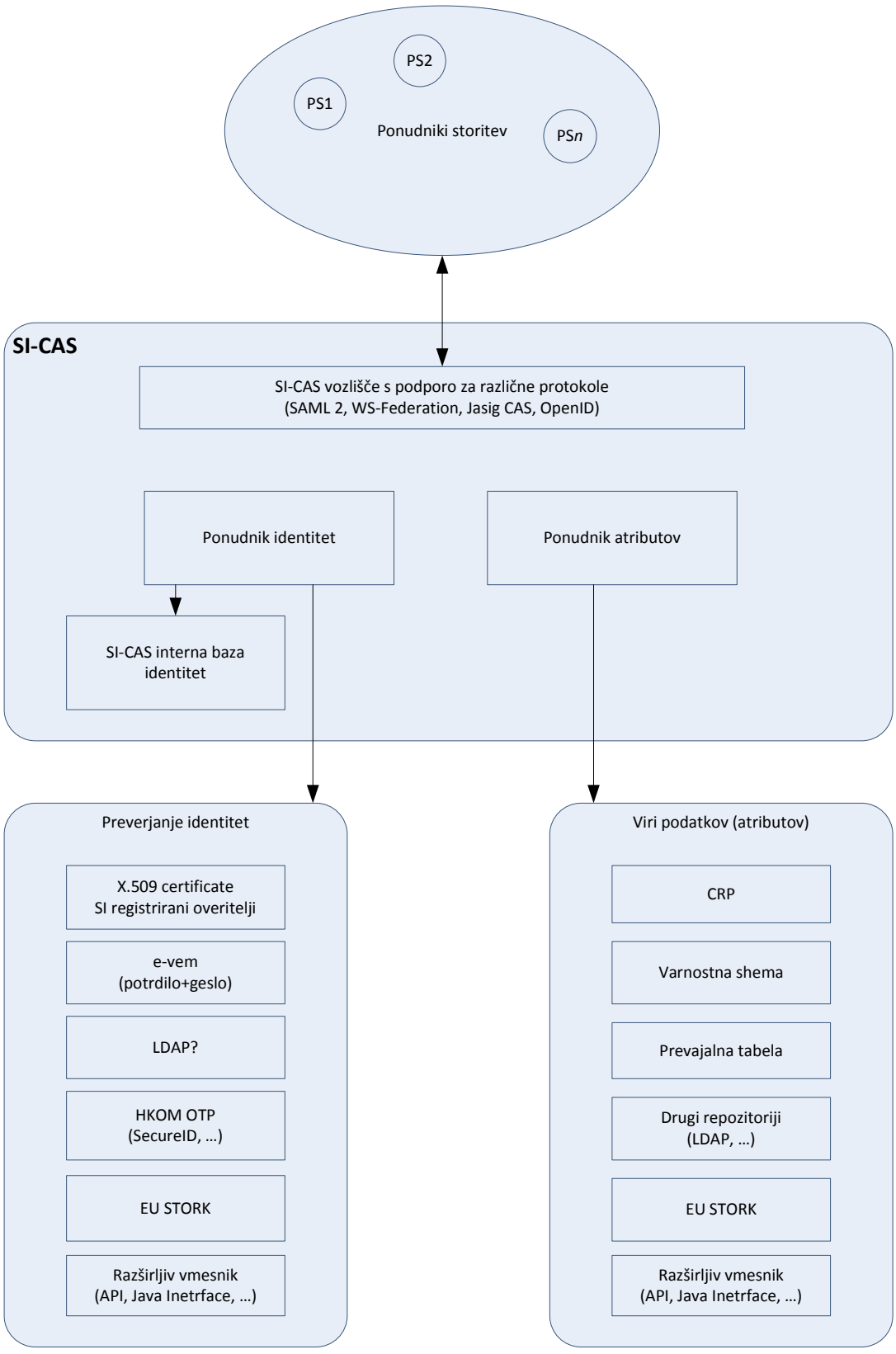
- Mehanizem avtentikacije uporabnikov: mehanizem avtentikacije, ki ga rešitev uporablja (uporabniška imena/gesla, digitalna potrdila, enkratna gesla, ...).
- Avtentikacijski mehanizem oziroma storitev: ali je avtentikacijski mehanizem vzpostavljen v okviru aplikacije ali pa se uporablja zunanja storitev.
- Identifikator, ki se uporablja za enolično prepoznavanje uporabnikov (interni identifikator ali zunanji identifikator, npr. davčna št., EMŠO, digitalno potrdilo, serijska številka potrdila, …).
- Subjekti, ki so končni uporabniki aplikacije.
- Uporaba več različnih avtentikacijskih mehanizmov: ali aplikacija omogoča uporabo različnih avtentikacijskih mehanizmov.
- Prva prijava, naslednje prijave: ali storitev za prvo prijavo in naknadne prijave uporablja isti postopek ali pa je prva prijava izvedena v smislu registracije, v okviru katere se zajame podatke o uporabniku, ki se nato shranijo v internem repozitoriju ponudnika storitve.
- Identifikacijski podatki (atributi), ki jih poleg identifikatorja potrebuje aplikacija pri prvi prijavi.
- Pridobitev, preverjanje, uporaba identifikacijskih podatkov ob naslednjih prijavah.
- Klasifikacija dostopnih pravic (varnostna shema) in pooblastila: ali se v okviru storitve dodeljujejo pooblastila uporabnikom; ali se uporablja varnostna shema in če da, katera instanca varnostne sheme.
- Prehod na SI-CAS identiteto: kateri postopek prehoda na SI-CAS identiteto je za ponudnika storitev sprejemljiv.
- Digitalni podpis: ali se v okviru aplikacije uporablja digitalni podpis in če se, katera oblika (XML, PDF, …), komponenta (npr. proXSign) in tip (npr. kvalificiran podpis).

Celoten vprašalnik za ponudnike storitev je dodan kot Priloga 2.

Na podlagi analize prejetih odzivov so bile oblikovane značilnosti oz. funkcionalne zahteve sistema SI-CAS, ki so podrobno predstavljene v nadaljevanju.

4 Značilnosti sistema SI-CAS

Sledeča slika prikazuje shemo komponent sistema SI-CAS:



V nadaljevanju je podan pregled zahtev za posamezne funkcionalne sklope SI-CAS.

4.1 Protokoli za upravljanje identitet

Podprti morajo biti vsaj naslednji protokoli za upravljanje identitet (oblika izmenjave zahtevkov/odgovorov med SI-CAS in ponudniki storitev):

- SAML verzija 2,
- Jasig CAS,
- opcijsko so lahko podprti tudi drugi protokoli npr. SAML verzija 1,WS-Federation, OpenID.

4.2 Upravljanje identitet SI-CAS

Pregled zahtev in omejitev zagotavljanja skupnega enoličnega identifikatorja v okviru SI-CAS:

- skupni identifikator ne more biti uveljavljeni ID npr. davčna številka, ker ga nimajo vse vključene identitete, zato se uvede baza identitet s posebnim SI-CAS ID, na katerega se povezujejo ostali UID-ji (Google in FB UID, davčna št. za dig. potrdila slovenskih izdajateljev, par serijska številka digitalnega potrdila in izdajatelj (SN-CA) za ostala digitalna potrdila, STORK ID...),
- zagotoviti je potrebno povezovanje identitet različnih prijavnih sistemov oziroma ponudnikov identitet,
- ponudnik identitet lahko vsem ponudnikom storitev posreduje isti identifikator ali pa vsakemu posreduje drugo vrednost[2].

Upravljanje identitet v okviru sistema SI-CAS mora omogočati:

- registracijo uporabnikov pri prvi prijavi v sistemu SI-CAS,
- dodeljevanje SI-CAS identitet uporabnikom ob njihovi registraciji,
- delovanje internega ponudnika identitet, ki novim uporabnikom omogoča registracijo uporabniških imen in gesel,
- podporo za različne ponudnike identitet, oz. identifikacijske mehanizme za avtentikacijo uporabnikov, in sicer vsaj sledeče:
  - kvalificirana digitalna potrdila v Sloveniji registriranih overiteljev,
  - kvalificirana digitalna potrdila overiteljev s sedežem v Evropski uniji, navedenih v zanesljivem seznamu overiteljev[3] (angl. Trusted Service List, TSL),

[2] Primer takega načina je SAML Persistent Identifier (“a persistent opaque identifier for a principal that is specific to an identity provider and a service provider or affiliation of service providers ”).

[3] https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

- digitalna potrdila overiteljev iz seznama korenskih izdajateljev v brskalnikih MS Internet Explorer in FireFox,
- digitalna potrdila overitelja ZZZS, shranjena na kartici zdravstvenega zavarovanja,
- internega ponudnika identitet,
- sistem za čezmejno avtentikacijo STORK,
- avtentikacijski mehanizem sistemov Facebook in Google,
- razširljiv vmesnik do poljubnih avtentikacijskih storitev (kot API ali Java vmesnik), ki omogoča podporo tudi za druge mehanizme npr. protokol LDAP za dostop do imenika uporabnikov, RSA SecureID, SMS avtentikacijo, RADIUS…

- povezovanje različnih identitet na zahtevo uporabnika,
- osnovni identifikatorji, povezani na uporabnikov SI-CAS ID, morajo biti ustrezno zaščiteni (z npr. ustrezno »hash« funkcijo),
- posredovanje različnih identifikatorjev na nivoju ponudnika storitev (SI-CAS za posamezen subjekt posreduje vsakemu ponudniku storitev drugo identiteto),
- filtriranje identifikacijskih mehanizmov na nivoju ponudnika storitev,
- filtriranje identifikacijskih atributov na nivoju ponudnika storitev,
- kategorizacijo identifikacijskih mehanizmov (varnostni nivoji in/ali profili),
- na zahtevo ponudnika storitev lahko odgovor vsebuje tudi podatek o identifikatorju uporabljenega identifikacijskega mehanizma npr. par SN-CA, STORK ID, RSA SecurID uporabniško ime…,
- opcijsko bi podprli tudi avtentikacijo aplikacije oz. servisa preko sistema SI-CAS v primeru, da se Varnostna shema uporablja tudi za upravljanje dostopnih pravic aplikacij.

Poleg zgoraj navedenih ponudnikov identitet oz. identifikacijskih mehanizmov bodo v sistem SI-CAS lahko kasneje vključeni tudi drugi novo vzpostavljeni (npr. avtentikacija preko mobilnih telefonov) ali obstoječi sistemi, kot so registri uporabnikov v okviru aplikacij (npr. Varnostna shema, e-Uprava in e-Vem), oziroma drugi zunanji sistemi. Obenem je potrebno predvideti možnost, da pride do sprememb pri delovanju oz. povezovanju z že vzpostavljenimi ponudniki identitet oz. identifikacijskimi mehanizmi.

Nivoji zaupanja v identiteto uporabnika se opredelijo z nivoji zaupanja ali kot profili. Nivo zaupanja oziroma profil odraža zaupanje v mehanizem preverjanja identitete ob registraciji in uporabljen identifikacijski mehanizem. V okviru profila mora biti omogočeno omejevanje digitalnih potrdil glede na:

- overitelja oziroma nabor overiteljev (npr. overitelji kvalificiranih potrdil registrirani v Sloveniji, overitelji kvalificiranih potrdil registrirani v EU, javni overitelji registrirani v brskalnikih, …),
- glede na vrsto potrdila, na primer kvalificirana potrdila za fizične osebe, za pravne osebe, …,
- glede na OID politike v potrdilu.

4.2.1 Registracija identitete, povezovanje identitet

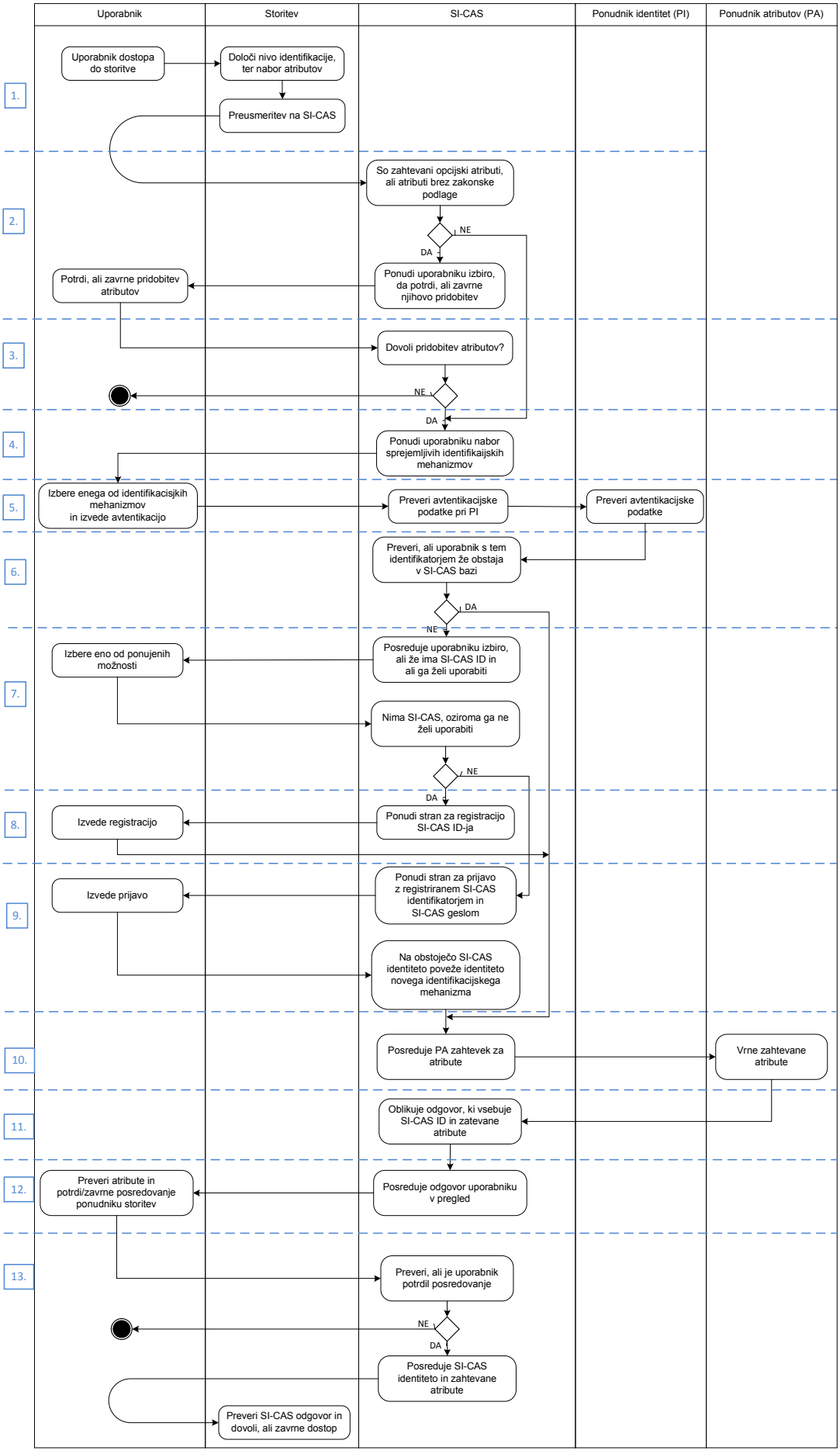
Uporabniki praviloma izvedejo registracijo identitete pri posameznem ponudniku identitet. Za potrebe dodeljevanja SI-CAS ID mora tudi SI-CAS omogočiti mehanizem in postopek registracije uporabnikov in identifikacijskih mehanizmov. Ker ima lahko uporabnik različne identifikatorje, to lahko predstavlja problem pri povezovanju identitet za istega uporabnika med različnimi ponudniki identitet. V okviru implementacije SI-CAS je potrebno zato predvideti mehanizem za povezovanje identitet, pri čemer uporabnik povezave med identitetami ureja sam preko SI-CAS portala, tako da se že prijavljen prijavi z drugo identiteto in tako naredi povezavo. Pri tem sta možna dva različna pristopa:

- uporabnik lahko registrira več različnih SI-CAS identitet in jih nato medsebojno poveže; slaba stran pristopa je, da bi v tem primeru moral SI-CAS ponudnikom storitev posredovati nabor povezanih SI-CAS identitet, kar lahko za slednje predstavlja precejšnjo spremembo,
- pri prijavi z novo identiteto ima uporabnik možnost le-to povezati na že obstoječo SI-CAS identiteto; slaba stran pristopa je, da ne omogoča naknadne povezave različnih SI-CAS identitet.

V sistemu SI-CAS se bo predvidoma uporabljal zadnji pristop, ki je podrobneje predstavljen v nadaljevanju.

4.2.2 Postopek prijave preko SI-CAS

Sledeča shema prikazuje koncept poteka prijave preko SI-CAS sistema. Posamezen korak prijave je opisan v nadaljevanju poglavja pod shemo.


Uporabnik
Storitev
SI-CAS
Ponudnik identitet (PI)
Ponudnik atributov (PA)
1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
Uporabnik dostopa do storitve
Določi nivo identifikacije, ter nabor atributov
Preusmeritev na SI-CAS
So zahtevani opcijski atributi, ali atributi brez zakonske podlage
NE
DA
Ponudi uporabniku izbiro, da potrdi, ali zavrne njihovo pridobitev
Potrdi, ali zavrne pridobitev atributov
Dovoli pridobitev atributov?
NE
DA
Ponudi uporabniku nabor sprejemljivih identifikaijskih mehanizmov
Izbere enega od identifikacisjkih mehanizmov in izvede avtentikacijo
Preveri avtentikacijske podatke pri PI
Preveri avtentikacijske podatke
Preveri, ali uporabnik s tem identifikatorjem že obstaja v SI-CAS bazi
DA
NE
Posreduje uporabniku izbiro, ali že ima SI-CAS ID in ali ga želi uporabiti
Izbere eno od ponujenih možnosti
Nima SI-CAS, oziroma ga ne želi uporabiti
NE
DA
Ponudi stran za registracijo SI-CAS ID-ja
Izvede registracijo
Ponudi stran za prijavo z registriranem SI-CAS identifikatorjem in SI-CAS geslom
Izvede prijavo
Na obstoječo SI-CAS identiteto poveže identiteto novega identifikacijskega mehanizma
Posreduje PA zahtevek za atribute
Vrne zahtevane atribute
Oblikuje odgovor, ki vsebuje SI-CAS ID in zatevane atribute
Posreduje odgovor uporabniku v pregled
Preveri atribute in potrdi/zavrne posredovanje ponudniku storitev
Preveri, ali je uporabnik potrdil posredovanje
NE
DA
Posreduje SI-CAS identiteto in zahtevane atribute
Preveri SI-CAS odgovor in dovoli, ali zavrne dostop

1. Ponudnik storitev določi zahtevani nivo/profil identifikacije ter nabor atributov (obvezni/opcijski, z/brez zakonske podlage); zahtevek se preko preusmeritve posreduje na SI-CAS.

2. V primeru, da zahteva vključuje tudi opcijske atribute ali atribute brez zakonske podlage, SI-CAS uporabniku izpiše seznam teh atributov in ga pozove, da potrdi njihovo pridobitev.

3. V primeru, da uporabnik ne dovoli pridobitve obveznih atributov brez zakonske podlage, se postopek ustavi.

4. SI-CAS na osnovi zahtevanega profila ter zahtevanega in odobrenega seznama atributov določi nabor sprejemljivih identifikacijskih mehanizmov in jih ponudi uporabniku.

5. Uporabnik izbere enega izmed ponujenih mehanizmov identifikacije in izvede avtentikacijo.

6. SI-CAS na podlagi identifikatorja uporabljenega identifikacijskega mehanizma (davčna št., SN-CA, STORK ID...) preveri, ali v interni bazi že obstaja zapis z registriranim identifikatorjem identifikacijskega mehanizma. Če zapis obstaja, SI-CAS vzame uporabnikov SI-CAS ID.

7. Če zapis ne obstaja, SI-CAS izpiše uporabniku naslednje obvestilo:

   ```
   V sistem SI-CAS ste se s prijavno metodo XXXXX prijavili prvič.
   Ali že imate uporabniški račun SI-CAS?
   Imam  -> Prijava
   Imam, a ga ne želim uporabiti  -> Registracija
   Nimam -> Registracija
   ```

8. Če uporabnik izbere registracijo, ga SI-CAS pozove, da vnese uporabniško ime, geslo in e-naslov, kreira nov uporabniški račun in mu dodeli SI-CAS ID ter na računu registrira identifikator identifikacijskega mehanizma.

9. Če uporabnik izbere prijavo, ga SI-CAS pozove, da se prijavi z obstoječim uporabniškim imenom in geslom SI-CAS, nakar na uporabnikovem računu registrira identifikator identifikacijskega mehanizma (t.j. na obstoječo SI-CAS identiteto poveže identiteto novega identifikacijskega mehanizma).

10. SI-CAS na osnovi atributov in/ali identifikatorja identifikacijskega mehanizma preko enega ali več ponudnikov atributov pridobi zahtevane atribute.

11. SI-CAS oblikuje odgovor, v katerega vključi SI-CAS ID ter vse pridobljene atribute (vsakega opremi z oznako obvezen/opcijski, zakonsko podlago ter oznako uporabljenega registra),

12. SI-CAS odgovor posreduje uporabniku in ga pozove, da pridobljene atribute pregleda, ter jih posreduje ponudniku storitve,

13. če uporabnik potrdi posredovanje podatkov, se odgovor SI-CAS prenese od uporabnika k ponudniku storitve.

4.3 Upravljanje atributov SI-CAS

Pregled zagotavljanja atributov v okviru SI-CAS:

- V okviru prenosa atributov bodo podprti osnovni atributi potrebni za identifikacijo uporabnika (ime, priimek, e-naslov, DŠ) ter nekateri dodatni atributi, ki jih potrebujejo posamezne aplikacije (datum rojstva, naslov, EMŠO, spol...).
- Prenos atributov bo odvisen od načina prijave:
  - pri prijavi z identitetami višjih nivojev (npr. kvalificiranimi digitalnimi potrdili) bo možno pridobiti atribute preko ponudnika atributov (npr. CRP) in jih posredovati aplikaciji,
  - pri prijavi z identitetami nižjih nivojev (npr. prijava z uporabniškim imenom ali preko sistema Facebook) se bodo posredovali le neposredno dostopni atributi (npr. ime, priimek, e-naslov).

Upravljanje atributov v okviru sistema SI-CAS mora omogočati:

- pridobitev atributov vsaj iz sledečih virov:
  - Centralni register prebivalstva (CRP),
  - Poslovni register Slovenije (PRS),
  - Evidenca zavarovancev ZZZS,
  - kadrovska evidenca zaposlenih v državnih organih,
  - Varnostna shema,
  - prevajalna tabela overitelja na MPJU,
  - sistem za čezmejno avtentikacijo STORK,
  - podatki iz digitalnega potrdila,
  - razširljiv vmesnik za dostop do poljubnih podatkovnih virov (kot API ali Java vmesnik),ki omogoča podporo tudi za druge repozitorije npr. protokol LDAP za dostop do imenika uporabnikov,baze podatkov SQL,…
- filtriranje nabora atributov, ki jih lahko zahteva ponudnik storitev oziroma se jih posreduje ponudniku storitev,
- filtriranje atributov glede na nivo identifikacijskega mehanizma (oziroma SI-CAS ob prijavi zahteva ustrezen nivo glede na zahtevane atribute),

- avtomatsko posredovanje atributov ponudnikom storitev, ki imajo zakonsko podlago; ponudnikom storitev, ki nimajo zakonske podlage, se posreduje atribute s posredovanjem uporabnika,
- pridobitev in združevanje atributov iz različnih virov, saj lahko odgovor, posredovan ponudniku storitev, vsebuje atribute, pridobljene iz različnih virov; v odgovoru mora biti za vsak atribut naveden tudi njegov vir (ponudnik atributov).

Zahteve glede integracije s prevajalno tabelo:

- podatki iz tabele (npr. davčna št. in EMŠO) se uporabijo le za vpogled v druge registre in se ne posredujejo ponudniku storitev kot atribut, razen če jih izrecno ne zahteva kot dodatne atribute,
- z namenom optimiziranega izvajanja vpogledov se že pridobljene podatke iz prevajalne lahko začasno shranjuje v okviru sistema SI-CAS.

Zahteve glede integracije z Varnostno shemo:

- SI-CAS mora podpreti možnost uporabe različnih Varnostnih shem za različne ponudnike storitev,
- SI-CAS mora podpirati integracijo z obstoječimi instancami Varnostne sheme.

4.4 Uporaba uradnih registrov

Osnovo za uporabo sistema SI-CAS bodo predstavljali dogovori med upravljavcem SI-CAS, upravljavci registrov ter ponudniki storitev, v katerih bodo določeni:

- institucija, odgovorna za delovanje SI-CAS,
- načini in pogoji dostopa do registra,
- kaj vse počne SI-CAS v imenu institucije,
- katera je pravna podlaga za dostop do osebnih podatkov za potrebe institucije,
  - maksimalni nabor podatkov, ki se bodo posredovali.

Predvidoma bosta omogočena dva načina posredovanja podatkov:

- Posredovanje podatkov na osnovi zakonske podlage: SI-CAS bo nastopal v vlogi posrednika med registrom in institucijo oz. informacijsko rešitvijo, ki potrebuje osebne podatke in zanje že ima ustrezno zakonsko podlago. Pri dostopu do registra bo možno posredovati tudi pravno podlago za dostop in/ali oznako institucije, v imenu katere se izvaja dostop.
- Posredovanje podatkov na osnovi uporabnikove zahteve: v primeru, da institucija nima pravne podlage za pridobivanje podatkov iz registra, uporabnik koristi SI-CAS za namene vpogleda v lastne osebne podatke, ki so shranjeni v registru. Od registra pridobljene podatke v obliki elektronskega izpisa uporabnik potem na osnovi svoje zavestne odločitve in izbire posreduje instituciji oz. informacijski rešitvi, kjer želi podatke uporabiti.

4.4.1 Centralni register prebivalstva

Kot atributi osebe se bodo iz registra CRP predvidoma prenašali naslednji podatki: EMŠO, davčna številka, spol, datum rojstva, kraj rojstva, prvi priimek, drugi priimek, vezaj, prvo ime, drugo ime, vezaj, naselje stalnega prebivališča, ulica stalnega prebivališča, hišna številka stalnega prebivališča, dodatek hišni številki stalnega prebivališča, poštna številka stalnega prebivališča, naziv pošte stalnega prebivališča, naziv državljanstva.

Iskanje se izvaja na osnovi davčne številke ali EMŠO uporabnika.

4.4.2 Poslovni register Slovenije

Kot atributi poslovnega subjekta se bodo iz registra PRS predvidoma prenašali naslednji podatki: naziv, skrajšani naziv, kraj, ulica, hišna št. poštna št., pošta, matična št., davčna št. in podatki o zakonitih zastopnikih.

Iskanje se izvaja na osnovi davčne in/ali matične številke poslovnega subjekta, ob prijavi zakonitega zastopnika kot uporabnika SI-CAS.

4.4.3 Evidenca zavarovancev ZZZS

Kot atribut osebe se bo iz registra ZZZS predvidoma prenašala le ZZZS številka.

Iskanje se izvaja na osnovi davčne številke ali EMŠO uporabnika.

4.4.4 Kadrovska evidenca zaposlenih v državnih organih

Kot atribut osebe se bo iz kadrovske evidence predvidoma prenašal podatek o instituciji, v kateri je oseba zaposlena.

Iskanje se izvaja na osnovi davčne številke ali EMŠO uporabnika.

4.5 Dodatni moduli in zahteve

4.5.1 Upravljanje sistema SI-CAS

Upravljavcem sistema SI-CAS bo za potrebe izvajanja osnovnih upravljavskih posegov na voljo grafični uporabniški vmesnik, katerega uporaba bo zahtevala ustrezno avtentikacijo upravljavca.

4.5.2 Integracija s ponudniki storitev

V okviru SI-CAS bo pripravljen modul za namestitev na strani ponudnikov storitev, ki mora imeti implementirane vse funkcije za povezovanje na SI-CAS in za dostop s strani aplikacije ponudnika storitev. Modul bo na voljo v tehnologijah Java in .NET.

4.5.3 Centralno preverjanje digitalnih potrdil

Ker digitalna potrdila predstavljajo prijavni mehanizem pri več ponudnikih identitet, ki bodo predvidoma vključeni v SI-CAS, bo v njegovem okviru vzpostavljen tudi mehanizem za preverjanje veljavnosti digitalnih potrdil, ki bo zagotavljal poenoteno preverjanje zaupanja v digitalna potrdila ter bo uporaben za validacijo potrdil vseh predvidenih ponudnikov identitet. Storitev validacije digitalnih potrdil bo poleg preverjanja veljavnosti potrdil omogočala tudi pridobivanje osnovnih identifikacijskih podatkov (atributov) iz digitalni potrdil. Ker bo vzpostavljena kot samostojni modul, bo kot centralna storitev na voljo tako SI-CAS kot predvidoma tudi drugim informacijskim sistemom oz. rešitvam. Za potrebe preverjanja kvalificiranih digitalnih potrdil bo storitev predvidoma uporabljala odprto-kodno rešitev Evropske komisije (DSS[4]).

4.5.4 Ostale zahteve

V nadaljevanju so podane še nekatere dodatne zahteve glede izvedbe SI-CAS:

- **Enkratna prijava**: sistem SI-CAS bo podpiral enkratno prijavo uporabnikov, pri čemer se bo posamezni ponudnik storitve lahko odločil, da za potrebe določene storitve enkratna prijava ni dovoljena in bo zato zahteval ponovno avtentikacijo uporabnika.

- **Varnostna shema:** ponudnik storitve bo imel možnost, da se ne odloči za uporabo integrirane varnostne sheme, temveč da bodisi integracijo z Varnostno shemo izvede izven SI-CAS bodisi uporabi svojo varnostno shemo.

- **Jezikovne različice:** spletne strani sistema SI-CAS, preko katerih se bo uporabnik registriral, avtenticiral ter povezoval svoje identitete, bodo dostopne v slovenskem in angleškem jeziku.

- **Uporaba HSM:** zaradi zagotavljanja ustreznega nivoja varnosti in zaupanja v sistem SI-CAS bodo kriptografski podatki in ključi sistema SI-CAS shranjeni na varnostnem strojnem modulu (HSM), na katerem se bodo izvajale vse kriptografske operacije, potrebne za delovanje sistema SI-CAS.

- **Zahteve za beleženje:** za potrebe omogočanja revizijskih sledi mora biti v okviru sistema SI-CAS vzpostavljen ustrezen način beleženja (logiranja) zahtevkov za avtentikacijo. Zaradi varovanja osebnih podatkov mora biti dostop do teh podatkov varovan v skladu z zahtevami zakonodaje s področja varovanja osebnih podatkov.

[4] https://joinup.ec.europa.eu/software/sd-dss/release/all

- **Zahteve po skalabilnosti:** zaradi pričakovanega postopnega naraščanja uporabe sistema SI-CAS in s tem njegove obremenitve mora slednji omogočati skalabilnost, tako da je mogoč enostaven prenos sistema oz. njegova vzpostavitev na drugi oz. dodatni strojni opremi.