SSI ALI SELF-SOVEREIGN IDENTITY V OKVIRU EVROPSKE UNIJE

Avtor: Gal Gracar

Visoka šola za poslovne vede

Povzetek

Posameznik kot produkt tako imenovanih brezplačnih storitev je problem, kateri bo v prihodnost postal pomembna tema obravnave v javnem diskurzu. Evropski parlament je v zavedanju tega problema postal mecen za novo tehnologijo, katera je trenutno še v razvojni fazi, vendar obljublja revolucionarno spremembo na področju posameznikove zasebnosti.

SSI, oziroma Self-Sovreign Identity je rešitev, katera temelji na blockchain tehnologiji, katera bo identiteo posameznika osvobodila verig digitalne dobe in postavila njegovo zasebnost in podatke na prvo mesto. Je tehnologija, katera mu bo omogočala, da bo lahko preko svoje blockchain naprave posredoval svoje zasebne podatke storitvam, katere jih bodo potrebovale (naprimer elektronska pošta ali prijava na katerkoli spletno stran). Posebnost te tehnologije pa ni samo to, da bo posamezniku omogočala varen prenos podatkov, temveč tudi to, da jih bo lahko posameznik zahteval nazaj. Zaradi svoje varnosti in praktičnosti bo v prihodnosti ta tehnologija omogočila, da bomo lahko za overjanje svoje identitete uporabljali izključno blockchain denarnico in ne več dosedanjih metod, kot so naprimer osebne izkaznice, potrdila o šolanju ali bančne kartice.

Podrobno smo opisali, kako bo SSI deloval, kakšni so njegovi ključni gradniki in zakaj je ta tehnologija tako varna. Poleg tega smo tudi ugotovili in predstavili vizijo EU, kako si le-ta želi, da bo ta sistem v prihodnosti deloval in katere vse zahteve za zaščito posameznikove varnosti bo ta tehnologija morala upoštevati.

Ključne besede: Self-Sovreign Identity, blockchain, zasebnost, EIDAS

Uvod

SSI je kratica, katera na kratko pomeni Self-Sovereign Identity in je rešitev za problematiko modernega sveta, v katerem je posameznik ujet v ekosistem internetnih gigantov, kateri razpolagajo z njegovimi podatki in nadzorujejo njegove podatke. Koncept SSI temelji na predpostavki, da je posameznik edini lastnik svoje identitete, katero nadzoruje in deli na način, ki mu omogoča najvišjo stopnjo avtonomije in zasebnosti. Posameznik lahko razkrije ali prikrije vse dele svoje identitete, katere želi in predstavi tretji strani samo podatke, katere ta potrebuje. *(Metadium, 2019)*

V trenutnem okolju je naša identiteta vezana na posamezne račune, katere imamo sklenjene z raznimi ponudniki e-storitev, tej pa potem z našimi podatki razpolagajo z našimi podatki, kateri se nahajajo v podatkovnih skladiščih ponudnikov. Ni pa potrebno, da si ustvarimo račun, da lahko tretja stran razpolaga z našo identiteto. Podatki o zaposlitvi, recepti, bančni podatki, podatki o plačilih in osebne izkaznice so samo eni izmed mnogih podatkov, ki o nas obstajajo in

so shranjene v podatkovnih bazah entitet, katerih sploh ne poznamo, kaj šele, da bi vedeli, kaj se dogaja z našimi podatki v ozadju.

V seminarski nalogi bomo preučili, kaj točno je SSI, kakšno je trenutno stanje njegovega razvoja in kako ga želi Evropska Unija s pomočjo EIDAS standard uvesti v naše življenje.

Kaj je SSI

SSI predstavlja našo identiteto na treh nivojih;

1. Kot posameznike, se pravi, naše ime, starost, kraj rojstva, zdravje, delovno mesto, navade, prepričanja in vse, kar nas kot posameznika oblikuje.
2. Digitalna dokazila, kot so osebne izkaznice, davčna številka, zgodovina naslovov, potrdila o delovni dobi, zdravstvena zgodovina,...
3. Interakcije naše identitete, kar pomeni vse situacije, v katerih smo morali predstaviti ali dokazati svojo identiteto, izvesti plačilo, overiti zavarovanja,... *(Gisolfi, et al, 2018)*

V Evropski Uniji je bil ustanovljen The European Union Blockchain Observatory and Forum, kateri poganja razvoj tehnologije blockchain in ekosistema blockchain, kar pomeni, da so neposredno vključeni v razvoj SSI v Evropski Uniji. Forum je sponzoriran s strani Evropske komisije, direktorat za omrežja, vsebino in tehnologijo. Maja 2019 je forum izdal poročilo Blockchain and digital identity, v katerem predstavi koncept Evropskega SSI in njegovih prednosti. Čeprav ni edini vključen v razvoj SSI, se bomo na njegovo poročili vrnili večkrat, saj je le-to ključnega pomena za nadaljnji razvoj SSI v Evropski uniji. *(Lyons, et al, 2019, 5-7)*

SSI mora po mnenju EU Blockchain Foruma vključevati več gradnikov, vsi pa so obvezni del naše identitete;

1. Decentralizirani identifikatorji (DID), kateri so nov tip identifikacije posameznika in njegove SSI. DID omogočajo popoln nadzor na svojo osebo. DID so za razliko od drugih identifikatorjev ustvarjeni izključno s strani uporabnika, kateri jih lahko ustvari toliko, kot jih potrebuje. Vsak DID dokazuje lastništvo osebe, katera ga lahko ustvari v poljubnih interacijah in nato po potrebi zbriše.
2. Dejanski podatki, katere bomo lahko posredovali drugim sistemom, ne glede na to, kakšen sistem bo v ozadju. Forum predvideva, da bo najpogostejša oblika za pošiljanje podatkov format JSON.
3. Hranjenje podatkov, katere lahko posameznik hrani ali na svoji elektronski napravi ali na oblaku, katerega si lahko posameznik izbere sam. Posameznik lahko podatke hrani v svoji osebni elektronski omarici, do katere mu nihče ne more omejiti dostopa. Posameznik lahko za potrebe interoperabilnosti uporabi podatke na več platformah hkrati in v vsakem primeru za različne namene. Na takšen način je nemogoče, da bi lahko bil posameznik priklenjen na samo eno platformo, to pa je ključno za osebnostno neodvisnost.
4. Varnostni ukrepi, kateri so vezani na decentraliziran sistem. Pri tem sistemu je varovanje podatkov stvar posameznika, ki se sam odloča, kakšne ukrepe bo izbral, kako jih bo izvedel in ali bo zaupal varstvo podatkov tretji osebi. To uporabniku predstavlja dodatno breme, saj je izključno na njem, da varuje svoje podatke, istočasno

pa to pomeni, da je povsem neodvisen od tretje strani, ki si varovanje podatkov lahko razlaga drugače.

5. Posrednik, kateri bo omogočal posamezniku, da generira svoje DID kode. *(Lyons, et al, 2019, 14-15)*

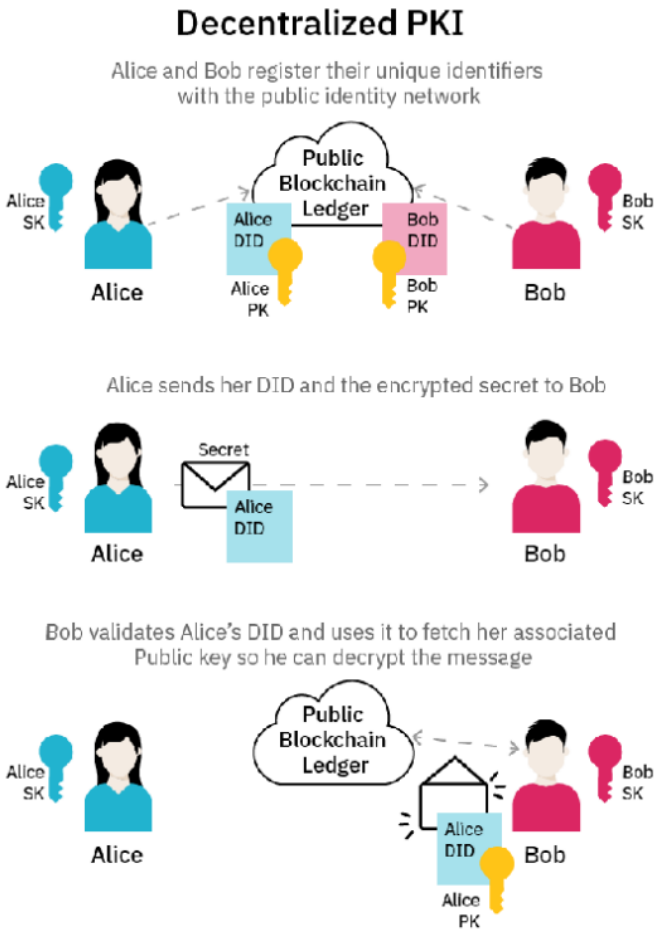
Končni namen SSI je decentralizacija posameznikove identitete, katera bi postala odgovornost posameznika in ne več posameznih podjetji, naprimer Google ali Facebook. Kljub temu je forum mnenja, da bo ISS identiteta še vedno odvisna od tretjih oseb, katere izdajajo podatke, naprimer izdajanje vozniških dovoljenj. Vozniška dovoljenja izda država in jih lahko tudi prekliče, če se pojavi potreba po tem. Kljub temu forum tega ne vidi kot slabost, saj bi bili tej podatki vezani na točno določen identifikator, kar izniči možnost zlorab ali napačnega vročanja.

Za konec forum še omenja, da bi nam decentralizirana identifikacija omogočala, da bomo lahko ustvarili različne persone glede na storitve, katere bomo uporabljali. Naša persona, ki bi jo videla zavarovalnica bi bila povsem drugačna od te, ki bi jo videla oseba na družbenem omrežju, saj bi vsaka persona vsebovala samo podatke, katere bi ji dovolili. *(Lyons, et al, 2019, 14-15)*

Kako delujeta SSI in DID

SSI model vsebuje podatke, kateri so izredno občutljivi, saj povedo vse o našem življenju. Da bi lahko varno izmenjavali podatke bi potrebovali najvišjo stopnjo varnosti. V ta namen je IBM predlagal rešitev vezano na blockchain tehnologijo, katero smo omenjali v prejšnjem poglavju. Blockchain omogoča kriptografsko izmenjavo podatkov iz ene naprave na drugo. Blockchain omogoča generacijo javnih ključev, kateri se generirajo po decentralizirani metodi.

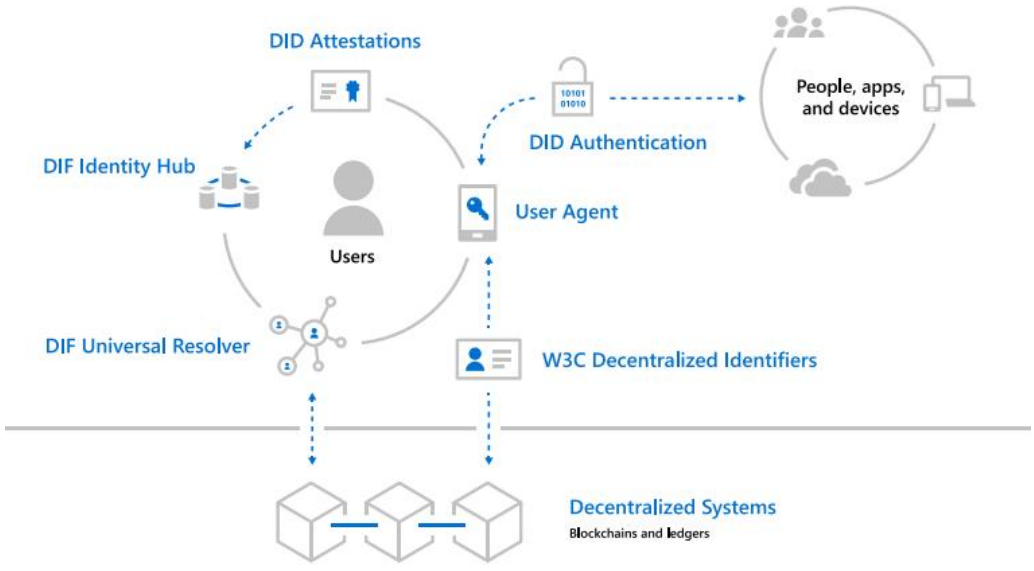
S pomočjo DID lahko oseba A pošlje osebi B željene podatke. Oseba B potrdi DID osebe A in ga uporabi, da pridobi javni ključ s pomočjo katerega lahko prebere podatke. *(Gisolfi, et al, 2018)*



Slika 1: Prikaz DPKI (Vir: IBM)

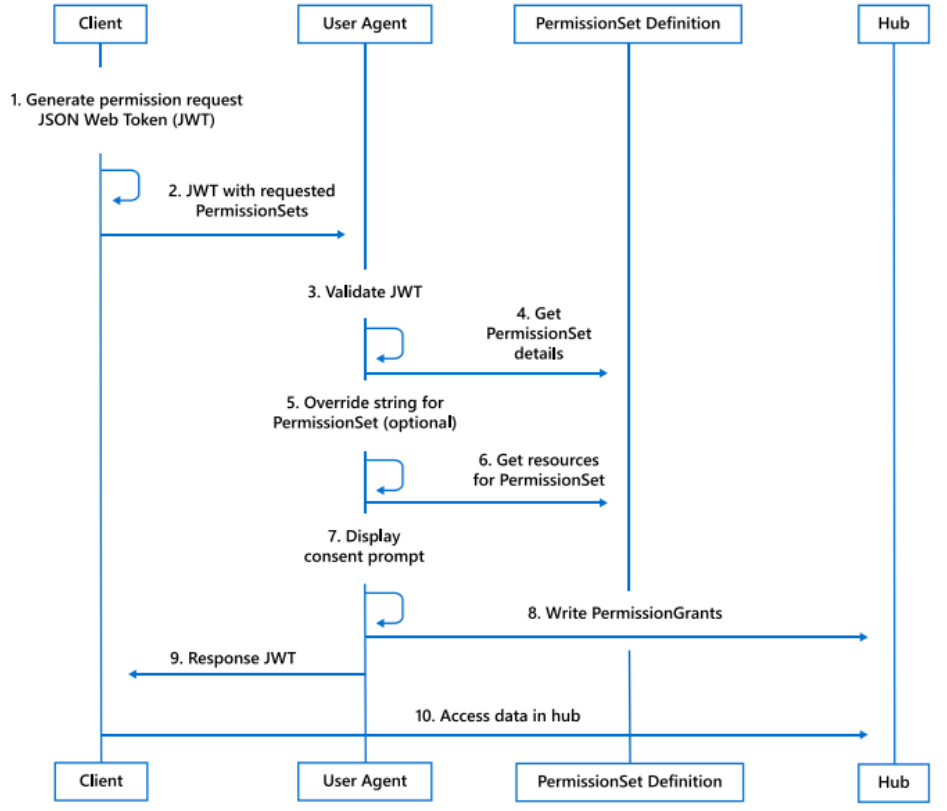
IBM pojasni več razlogov, zakaj za SSI stoji tehnologija blockchain. Pomemben faktor so informacije, ki razkrijejo našo osebnost (PII -personally identifiable information). Blockchain lahko hrani podatke razpršeno, vendar je več kot samo to. S pomočjo DID identifikatorjev blockchain mapira podatke na podoben način, kot DNS mapira internet; ustvari unikatne povezave do osebe, entitete ali povezane naprave. Kljub temu DID ne povezuje overilnic, katere se nikoli ne nahajajo v javni domeni. S pomočjo potrjenih kriptografskih P2P povezav lahko DID poveže tajne podatke z osebo, ki jih želi videti, to pa stori tako, da mu pošlje ključ do podatkov, nakar jih dekodira in overi. *(Gisolfi, 2018)*

DID se počasi uveljavlja kot rešitev za decentralizirano identiteto. DID je univerzalno vezan na blockchain rešitev in počasi že vidimo napredek na tem področju. Microsoft je v navezi s W3C predstavil svojo vizijo v poročilu Decentralized Identity leta 2018. *(Microsoft Corporation, 2018, 7)*



Slika 2: Delovanje DID (Vir: Microsoft)

- S pomočjo W3C decentraliziranih identifikatorjev lahko uporabnik ustvari, poseduje in upravlja s svojimi decentraliziranimi javnimi ključi kot želi in to neodvisno od katerekoli druge organizacije ali vlade. Decentralizirana infrastruktura javnih ključev (DPKI) sestoji iz JSON dokumentov, kateri vsebujejo materiale javnih ključev, deskriptorje avtentikacije in končne točke storitve.
- Decentralizirani sistemi, kar so ponavadi blockchain rešitve, nudijo mehanizme, kateri so potrebni za dostop do DPKI. Microsoft razvija standarde in tehnologije s pomočjo blockchain skupnosti, kar bo omogočilo čim večjo raznolikost blockchainov in imenikov.
- Uporabniški agenti DID so aplikacije, ki omogočajo posamezniku, da uporabi svojo decentralizirano identiteto. Ustvarjajo DIDe, upravljajo s podatki, dovoljenji in overjujejo zahtevke DID.
- Univerzalni DIF razreševalnikvsebuje zbirko DID gonilnikov s katerim omogoča poizvedbe in razrešitve za DID na različnih implantacijah in decentraliziranih sistemih. Ko dobi ukaz za poizvedbo, vrne DID Document Object (DDO), kateri vsebuje DPKI metapodatke, ki so vezani na DID.
- Identifikacijski hubi DIF so ponovljene zbirke enkriptiranih osebnih zbrik podatkov, ki so vezani na naprave, kot so telefoni, računalniki in drugi. Hranijo podatke identitete in podatke, kjer se je identiteta uporabljala.
- DID dokazila (attestations) so standardni formati in protokoli, ki omogočajo lastnikom identitete, da ustvarijo predstavijo in overijo zahtevke. To ustvari nivo zaupanja med uporabniki v sistemu.
- Decentralizirane aplikacije in storitve, vezane na identifikacijske hube in osebne zbirke podatkov. Hranijo podatke s pomočjo uporabnikovega huba in delujejo v sklopu dovolilnic, katere je uporabnik dovolil. *(Microsoft Corporation, 2018, 8-10)*



Slika 3: Potek dovoljenji za podatkovni dostop (Vir: Microsoft)

Identifikacijski hubi omogočajo hrambo in posredujejo sporočila, nimajo pa ključev za odklep podatkov. Uporabniki lahko brez težav umaknejo dostop do podatkov vsakomur. Dovoljenja so podpisana z DID ključi, podatki pa so zaščiteni na način, kot ga ključi zahtevajo. *(Microsoft Corporation, 2018, 18)*

SSI in EU - Vizija

Za namen vpeljave SSI v javno življenje, je Evropska komisija v sodelovanju z European Blockchain Partnership razvila iniciativo European Blockchain Services Infrastructure. Leta 2019 je iniciativa pričela s selekcijo prvih primerov prakse, v začetku leta 2020 pa je objavila prve izsledke teh primerov prakse. *(EBSI, 2020)*

SSI je bila ena izmed prvih fraz, ki jih lahko zasledimo v izredno izčrpnem poročilu o primerih prakse. Poročilo omenja več področji, kjer ima SSI velik potencial;

- Javni sektor:
    - Potovanje in priseljevanje; hramba dokumentov, potrebnih za mednarodno potovanje, zmanjšanje obsega dela preverjanja podatkov, hitrejše procesiranje

primerov iz tednov na minute, izničenje možnosti goljufije ali ponarejanja dokumentov.
    - Šolska potrdila; predlog prenosa vseh diplom, certifikatov, podatkov o šolanju v SSI sistem, kar bi dodatno zmanjšalo možnosti za prevaro, ter olajšalo posamezniku prijavo na univerzo ali delovno mesto.
    - Javne dovolilnice; hramba dovolilnic ali dovoljenj, kot so vozniško dovoljenje, licence za določena dela, z možnostjo preklica s strani izdajalca dokumenta.
    - Zaposlitveni podatki; podatki o delovni dobi, socialni transferji, dovoljenja za najem kredita ali lizinga …
    - Zdravstvene kartice in recepti; SSI lahko olajša posamezniku prenos zdravstvenih kartotek, ter omogoči čim manj podpisovanja dokumentov. Namen je tudi, da bo SSI dovolil hrambo receptov in njihove zgodovine.
    - Parkiranje in javni prevoz; hramba dovolilnic, kot so Urbana, potrdila o parkirnih mestih, mesečne vozovnice…
    - Podatki o članstvih; članstva vezana na status posameznika (upokojenec, študent, invalid…)
    - Potrdilo o prejemkih ali subvencijah, prijavah na javne razpise; zgodovina javnih prejemkov in zgodovina prijavljenih ali opravljenih javnih razpisov. SSI bo olajšal takšne prijave in jih pohitril.
    - Podatki o rojstvu, smrti ali dokazilih o obstoju; Dokazila o obstoju ali smrti bodo olajšala potrditev identitete in bodo preprečevala napake, pri katerih so morali ljudje dokazovati, da niso mrtvi.

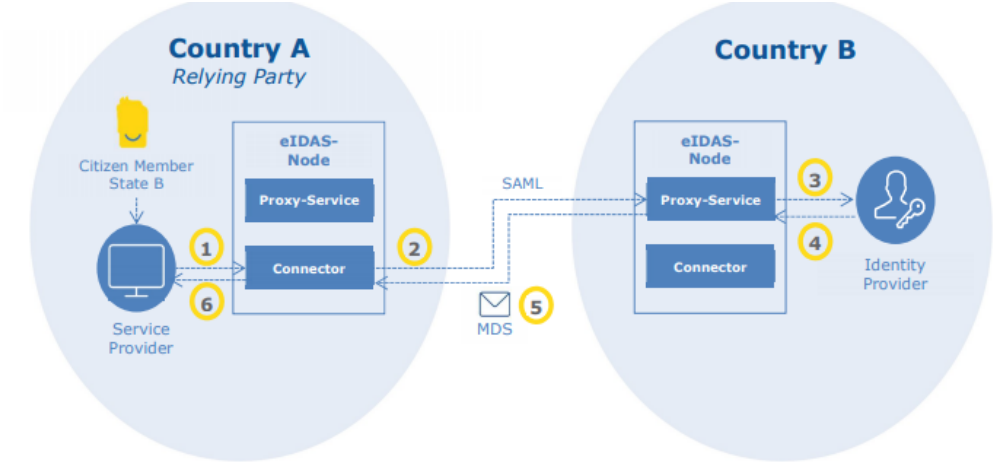
- Zasebni sektor:
    - Dostop do omrežnih storitev; hramba gesel, uporabniških imen in avtentifikacij.
    - Know your customer / Anti-Money Laundering; posameznik se lahko dokaže s pomočjo SSI sistema na banki ali poslovalnici, brez, da bi moral narediti vmesni korak preko overjevalca identitete.
    - Upravljanje in dostop do podatkov; trenutni sistemi identitete in dostopa do podatkov (IAM) so zelo kompleksni, centralizirani in izredno dragi. SSI rešitev bi lahko povsem odpravila z njimi.
    - Dostop do finančnih in zavarovalniških storitev; SSI omogoči sklepanje storitev v krajšem času in izniči proces pridobivanja in overjevanja dokumentov.
    - Spletno nakupovanje in trgovina; olajšanje plačevanja v trgovini ali preko spleta.
    - Dostava; SSI omogoča dostavo na točen naslov in olajša proces identifikacije pri dostavi ali carini.
    - Kartice zvestobe in CRM; Kartice zvestobe in CRM orodja se močno omeji s podatki, katere jim dovolimo, da vidijo. *(EBSI, 2020, »ESSIF how we use SSI)*

SSI in EIDAS

Maja 2019 je inštitut Evropske komisije eIDAS Observatory objavil članek vizije povezanega SSI modela s eIDAS sistemom. *(Gomez Munoz, 2019, 1)*

Regulacije eIDAS bi zagotovile, da bi se lahko ljudje in pravne osebe povezale s katerimi koli drugimi inštitucijami v EU. Notranji evropski trg bi prav tako zagotovil tudi, da bi sistem lahko deloval onkraj meja EU in posedoval enak pravni status, kot papirnati dokumenti. Dokumenti, pridobljeni preko SSI bi imeli pravno podlago in bi jih bilo nemogoče zavrniti na podlagi svoje elektronske oblike. Status nediskriminatorne politike bi obsegal vse oblike dokumentov, ne glede na to, ali so tekstovni, vizualni ali zvočni.

Pravila eIDAS zagotavljajo, da bi spletne storitve morale overiti vsako zahtevo po verifikaciji elektronskih dokumentov. Ta pravila bi veljaja za javni sektor, medtem, ko bi zasebni sektor lahko takšne dokumente priznal prostovoljno. *(Gomez Munoz, 2019, 3)*



Slika 4: Elektronska identifikacija preko eIDAS (Vir: Gomez Munoz)

EIDAS bi pomenil tudi večjo raven zaupanja na petih nivojih, katere ureja:

- Elektronski podpis
- Elektronski žig
- Elektronski časovni žig
- Spletni overilni certifikati (Website Authentication Certificates – WAC)
- Elektronski dostavni register (Electronic Registered Delivery Service)

Poleg tega eIDAS ureja tudi tri tipe podpisov ali žigov;

- Preprosti; vezan na podpisan dokument ali podatke, katere želi podpisovalec overiti, ponavadi skeniran fizični podpis.
- Napredni; elektronski podpis, ki je unikatno povezan s podpisnikom in beleži nadaljnje spremembe dokumentov.
- Kvalificirani; napredni elektronski podpis, ki je podprt s certifikatom, za katerim stojijo overjevalne službe. Prav tako je ustvarjen s pomočjo napredne naprave za izdelavo podpisov, katera mora zagotavljati visoko stopnjo varnosti med izdelavo podpisa.

Kvalificirani elektronski podpisi imajo enako pravno podlago kot ročni podpisi in velja v vseh državah EU, katere morajo poskrbeti, da se tako kvalificirani, kot napredni podpis, držijo ETSI standardov (ASiC, PAdES, CAdES, XAdES). *(Gomez Munoz, 2019, 4-5)*

EIDAS bi zagotavljaj tudi povezavo identitete z DID, in sicer na dva načina; Prvič s avtentifikacijo s pomočjo eID sheme, ko je potrebno izvesti prijavo na spletne storitve. In pa drugič z izdelavo elektronskega podpisa ali žiga, ko se podpisnik rabi poistovetiti s podpisanim ali ožigosanim dokumentom. V obeh primerih bi eIDAS zagotovil povezavo DID s dejansko identiteto lastnika DID. *(Gomez Munoz, 2019, 6)*

Zaključek

SSI je nova in mlada tehnologija, ki je še v povojih, vendar obljublja, da bo spremenila svet. Mobilnost, ki je danes ključnega pomena za obstoj napredne in digitalne družbe, bo s pomočjo SSI prišla na novo raven, hkrati pa bo prinesla s seboj nov koncept zasebnosti. Človek bo postal popolnoma neodvisen od spleta za hrambo svojih zasebnih podatkov in praktično neviden za vse korporacije, katere trenutno služijo z njegovimi podatki. Ker pa je žal ta tehnologija zaenkrat še v konceptni fazi z omejenimi poskusnimi fazami, ni pričakovati, da bo stopila v veljavo prav kmalu. Kljub temu pa je ta tehnologija uspela usmeriti pozornost nase in dogajajo se resni premiki, kateri jo bodo počasi iz koncepta premaknili v pilotsko fazo, katera bo vsekakor osupljiva in bo radikalno spremenila to, kako gledamo na zasebnost in na mobilnost.

Viri in literatura

Metadium, Introduction to Self-Sovereign Identity and Its 10 Guiding Principles, 2019

D. Gisolfi, M. Patel, R. Radulovich, Decentralized Identity Introduction. IBM Corporation, 2019

T. Lyons, L. Courcelas, K. Timsit, Blockchain and Digital Identity. The European Blockchain Observatory and Forum, 2019

D. Gisolfi, Self-sovereign identity: Why blockchain? IBM Corporation, 2018

Decentralized Identity. Microsoft Corporation, 2018

European Blockchain Services Infrastructure (EBSI). [2020]. The 2019 EBSI use cases. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI

European Blockchain Services Infrastructure (EBSI). [2020]. ESSIF How we use SSI. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+How+we+use+SSI#ESSIFHowweuseSSI-Introduction

C. Gomez Munoz, SSI and eIDAS: a vision on how they are connected. 2019