



REPUBLIKA SLOVENIJA

MINISTRSTVO ZA NOTRANJE ZADEVE

DIREKTORAT ZA INFORMATIKO IN E-STORITVE

Tržaška 21, 1000 Ljubljana



Naložba v vašo prihodnost

OPERACIJO DELNO FINANCIRA EVROPSKA UNIJA
Evropski socialni sklad



Slovenia
Business Point

Centralni (strežniški) e-podpis Funkcionalne specifikacije

Naloga:

Priprava funkcionalnih specifikacij za centralni (strežniški) e-podpis za operacijo »Enotna kontaktna točka 2 – Vzpostavitev elektronskih postopkov poslovnega portala (EKT2)«.

STANJE DOKUMENTA

Namen:	Funkcionalne specifikacije za centralni (strežniški) e-podpis
Vsebina:	Vsebina dokumenta je vidna iz kazala.
Oznaka:	EKT2-CeS-FS
Status:	Končna verzija za potrjevanje
Verzija:	1.0
Datum verzije:	8. avgust 2013
Stanje:	Dokument ni lektoriran.
Lastnik:	Ministrstvo za notranje zadeve, Direktorat za informatiko in e-storitve
Avtorji:	JAB d.o.o.

ZGODOVINA SPREMEMB

Verzija	Datum	Razlog za spremembe	Spremenil
V 0.0	26.05.2013	Prva delovna verzija	Boštjan Jaklič
V 0.1	06.06.2013	Prilagoditve glede na sestanek 31.05.2013	Boštjan Jaklič
V 0.2	08.06.2013	Dopolnjena poglavja od 2.3 naprej	Boštjan Jaklič
V 0.3	01.07.2013	Dodani opisi za avtomatsko registracijo, prilagoditve ostalih opisov	Boštjan Jaklič
V 0.4	15.07.2013	Umaknjeni opisi za primer, ko ima uporabnik za vsak podpis drug zaseben ključ. Dopolnjen opis overitelja.	Boštjan Jaklič
V 0.5	30.07.2013	Ločen opis upravljanja digitalnih potrdil za avtentikacijo i digitalni podpis	Boštjan Jaklič
V 0.6	02.08.2013	Preverjanje veljavnosti digitalnega podpisa prestavljeno iz dodatnih storitev v poglavje 2.6.3 Preverjanje veljavnosti e-podpisa	Boštjan Jaklič
V 1.0	08.08.2013	Vnešene pripombe s sestanka 7.8.2013	Boštjan Jaklič

KAZALO

1	Uvod	5
1.1	Namen in cilji	5
1.2	Centralni (strežniški) e-podpis in projekt EKT2	6
2	Funkcionalne zahteve	8
2.1	Centralna storitev e-podpisa s ključi imetnika	10
2.2	Uporabniški kriptografski ključi in digitalna potrdila	11
2.2.1	Digitalno potrdilo za avtentikacijo	12
2.2.2	Digitalno potrdilo za e-podpis	13
2.2.3	Dodatne zahteve	13
2.3	Avtentikacija ob uporabi storitve SI-CeS.....	14
2.3.1	Nivoji SI-CAS avtentikacije in e-podpisa	15
2.4	Upravljanje življenjskega cikla ključev in digitalnih potrdil imetnikov	16
2.4.1	Upravljanje digitalnih potrdil za avtentikacijo.....	17
2.4.1.1	Registracija uporabnikov	17
2.4.1.2	Prva aktivacija uporabnikov in potrdil na SI-CeS	17
2.4.1.3	Obnova potrdila	17
2.4.1.4	Upravljanje uporabnikov sistema SI-CeS.....	17
2.4.1.4.1	Sprememba uporabniškega gesla	18
2.4.1.4.2	Ponastavitev pozabljenega uporabniškega gesla.....	18
2.4.1.4.3	Ukinitev (odjava) storitve.....	18
2.4.1.4.4	Preklic digitalnega potrdila	19
2.4.2	Upravljanje digitalnih potrdil za digitalni podpis.....	19
2.4.2.1	Registracija uporabnikov	19
2.4.2.2	Prva aktivacija uporabnikov in potrdil na SI-CeS	19
2.4.2.3	Obnova potrdila	19
2.4.2.4	Upravljanje uporabnikov sistema SI-CeS.....	20
2.4.2.4.1	Sprememba uporabniškega gesla	20
2.4.2.4.2	Ponastavitev pozabljenega uporabniškega gesla.....	20
2.4.2.4.3	Ukinitev (odjava) storitve.....	20
2.4.2.4.4	Preklic digitalnega potrdila	20
2.4.3	Dodatni vidiki upravljanja digitalnih potrdil in uporabniških ključev	20

2.5 Varovanje zasebnih ključev imetnikov	21
2.5.1 Varna hramba zasebnih ključev	21
2.5.2 Aktiviranje/de-aktiviranje uporabniških ključev ob uporabi storitve.....	21
2.6 Tehnične zahteve e-podpisa.....	22
2.6.1 Oblike vhodnih podatkov za podpis	22
2.6.2 Oblike e-podpisa SI-CeS.....	22
2.6.3 Preverjanje veljavnosti e-podpisa	23
2.6.4 Dodatne storitve	23
2.7 Operativne in varnostne zahteve	24
2.7.1 Aktiviranje kriptografskih ključev	24
2.7.2 Strojni varnostni moduli (HSM).....	24
2.7.3 Zahteve za beleženje	24
Dodatek – kratice in pojmi	25
Kratice	25
Pojmi	25

1 Uvod

Projekt »Enotna kontaktna točka 2 – Vzpostavitev elektronskih postopkov poslovnega portala« (na kratko EKT 2) bo skupaj z operacijo EKT 1 (Enotna kontaktna točka: vzpostavitev poslovnega portala – informacijski del) vzpostavila poslovni portal, ki bo obstoječim in bodočim poslovnim subjektom nudil celovite informacije in elektronsko podporo urejanju vseh formalnosti, ki jih poslovni subjekti potrebujejo za svoje poslovanje oz. opravljanje storitev.

Vzpostavitev storitve za centralni (strežniški oz. »cloud«) e-podpis (v nadaljevanju SI-CeS) v okviru projekta EKT 2 bo namenjena integraciji funkcionalnosti elektronskega podpisovanja za potrebe opravljanja elektronskih storitev, pri katerih se zahteva elektronsko podpisovanje dokumentov.

1.1 Namen in cilji

V obstoječih rešitvah e-podpisovanja se uporabljajo rešitve, ki temeljijo na integraciji podpisne programske opreme (komponente) v posamezne odjemalce (npr. brskalnike), kar pa ne predstavlja optimalnega pristopa iz več vidikov:

- upravljanje programske opreme je zahtevno, saj vključuje vzdrževanje podpisnih komponent za veliko število platform (operacijski sistem in brskalnik),
- dodajanje novih funkcionalnosti je počasnejše, ker je potrebno nadgrajevati več različnih komponent,
- e-podpisovanje je omejeno na platforme, ki podpirajo uporabo digitalnih potrdil,
- oteženo je čezmejno e-podpisovanje s strani uporabnikov iz drugih držav članic EU, kar je bistvenega pomena zaradi zahtev storitev EKT 2 po zagotavljanju delovanja notranjega trga EU.

Cilj projekta je izdelava funkcionalnih specifikacij sistema za elektronski podpis s ključi imetnikov digitalnih potrdil na SI-CeS. Storitve centralnega (strežniškega) e-podpisa s ključi imetnikov bo temeljila na sledečih izhodiščih:

- Zasebni ključi uporabnikov bodo hranjeni na centralnem sistemu. Dostop do zasebnih ključev bo zaščiteno z uporabo stojnih varnostnih modulov (v nadaljevanju HSM, angl. Hardware Security Module) in bo tako v največji možni meri onemogočena nepooblaščen uporaba zasebnih ključev.

- Vsak uporabnik SI-CeS storitve bo lahko imel digitalna potrdila dveh tipov. Eno ali več potrdil za e-podpis in eno digitalno potrdilo za avtentikacijo v povezavi z avtentikacijo preko centralnega avtentikacijskega sistema (v nadaljevanju SI-CAS) na osnovi dvo-faktorske identifikacije z uporabo SMS OTP¹ in uporabniškega gesla.
- Identifikacija uporabnikov se bo izvajala preko SI-CAS, ki bo prav tako razvit v okviru projekta EKT 2².
- Kot uporabniško geslo za odobritev uporabe uporabniških ključev na SI-CeS se uporablja SI-CAS geslo.

Storitev za centralni (strežniški) e-podpis bo prilagodljiva in bo podpirala različne možnosti pri izvedbi e-podpisa:

- omogočeno bo tvorjenje e-podpisa v skladu z različnimi standardi oz. formati (binarni, XML, PDF, CMS);
- podprto bo oblikovanje e-podpisa različnih nivojev (kvalificiran e-podpis, napreden e-podpis overjen s kvalificiranim potrdilom, napreden e-podpis);
- uporabniku bo na voljo več možnosti avtentikacije pri tvorbi e-podpisa glede na zahtevani nivo e-podpisa ter glede na mehanizme avtentikacije, ki jih bo podpiral SI-CAS.

Storitev bo omogočala varen e-podpis brez nameščanja podpisnih komponent na strani uporabnika, kar bo omogočilo uporabo e-podpisa v vseh uporabniških okoljih, tako stacionarnih kot mobilnih. Neodvisnost storitve e-podpisa od uporabniškega okolja bo tako med drugim omogočila uvajanje storitev e-podpisa v oblaku.

Storitev za centralni (strežniški) e-podpis bo kot centralna funkcija na voljo tudi drugim storitvam e-uprave. Zahtevana oblika in nivo podpisa bosta glede na občutljivost e-storitve določena s strani ponudnika posamezne e-storitve, ki bo uporabljala storitev za centralni (strežniški) e-podpis.

1.2 Centralni (strežniški) e-podpis in projekt EKT2

Direktiva 2006/123/ES o storitvah na notranjem trgu (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

¹ SMS OTP – tekstovno sporočilo z enkratnim geslom (angl. One Time Password sent over Short Message Service)

² V času priprave pričujočega dokumenta SI-CAS še ni vzpostavljen, funkcionalne specifikacije so v dokumentu [EKT2-CAS]-Funkcionalne specifikacije in tehnična zasnova_v1.1.pdf

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 dovoljenj, 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 tudi vzpostavitev horizontalnih/centralnih funkcij skladno z Akcijskim načrtom e-poslovanja javne uprave (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 uvedli 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 za avtomatski prenos vsebine oz. opisov od pristojnih institucij do EKT, centralno storitev za avtentikacijo (SI-CAS), ter nenazadnje vzpostavitev storitve centralnega (strežniškega) e-podpisa s ključi imetnikov digitalnih potrdil, ki je predmet pričujočih funkcionalnih specifikacij.

2 Funkcionalne zahteve

Elektronski podpis mora zagotoviti možnost povezave podpisa na elektronskem dokumentu s fizično osebo, ki je podpis kreirala, možnost preverjanja integritete podpisa ter ugotavljanja identitete podpisnika. Pri uporabi X.509 digitalnih potrdil so te zahteve izpolnjene z uporabo kriptografskih ključev, kriptografskih algoritmov ter digitalnih potrdil izdanih s strani zaupanja vrednih overiteljev. Pri elektronskih podpisih z uporabo digitalnih potrdil so zahteve elektronskega podpisa zagotovljene na sledeč način:

- Identiteto podpisnika je možno ugotoviti iz digitalnega potrdila podpisnika. Zaupanje v identiteto podpisnika izhaja iz zaupanja v overitelja digitalnih potrdil, ki je digitalno potrdilo izdal.
- Možnost preverjanja integritete podpisanih podatkov in podpisa je zagotovljena z uporabo kriptografskih algoritmov in podpisnikovega javnega ključa, vsebovanega v digitalnem potrdilu. Zaupanje v javni ključ oz. pripadnost javnega ključa podpisniku izhaja iz zaupanja v overitelja, ki je izdal digitalno potrdilo.
- Možnost preverjanja, da je elektronski podpis res kreiral imetnik digitalnega potrdila, je zagotovljena z uporabo asimetričnih kriptografskih ključev. Preverjanje veljavnosti podpisa z javnim ključem, vsebovanim v digitalnem potrdilu, bo uspešna le v primeru, če bo podpis kreiral imetnik pripadajočega zasebnega ključa. Nivo zaupanja v verodostojnost podpisa je tako odvisna od nivoja varovanja zasebnega ključa podpisnika, oziroma zaupanja, da je zasebni ključ izključno pod nadzorom podpisnika.

Opomba: V zgornjih alinejah je naveden le pregled elementov elektronskega podpisa relevantnih za funkcionalno specifikacijo storitve centralnega (strežniškega) e-podpisa.

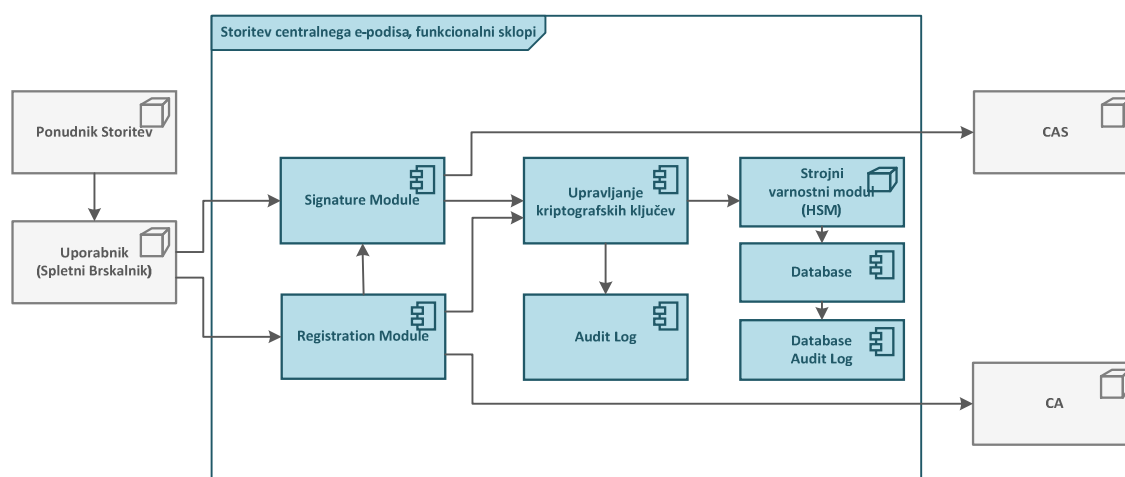
Storitev centralnega (strežniškega, »cloud«) e-podpisa s ključi imetnikov v osnovi izpolnjuje vse zgoraj navedene elemente zaupanja v elektronski podpis. Bistvena razlika v primerjavi s splošno uveljavljenimi rešitvami je način zagotavljanja, da je »zasebni ključ izključno pod nadzorom podpisnika«. Splošno uveljavljen način izpolnjevanja zahteve, da je »zasebni ključ izključno pod nadzorom podpisnika«, temelji na varni hrambi in uporabi zasebnega ključa pri uporabniku. Ključna funkcionalna zahteva storitve centralnega (strežniškega) e-podpisa s ključi imetnikov je zagotavljati enak nivo zaupanja v elektronski podpis, oziroma zaupanja, da je »zasebni ključ izključno pod nadzorom podpisnika«, kot ga zagotavljajo uveljavljene rešitve. Varnost zasebnih ključev imetnikov na centralnem sistemu mora biti zagotovljena s tehničnimi mehanizmi, organizacijsko-operativnimi ukrepi ter postopki upravljanja življenjskega cikla kriptografskih ključev in digitalnih potrdil (več o tem v dokumentu »Analiza skladnosti za uvedbo varnejših in uporabniku prijaznejših e-identitet,

Priloga B«, dostopno na <https://nio.gov.si/nio/asset/analiza+moznosti+za+uvedbo+varnejshi+in+uporabniku+prijaznejsh+eidentitet>).

V nadaljevanju dokumenta so podane funkcionalne zahteve storitve centralnega (strežniškega) e-podpisa SI-CeS za sledeče segmente:

- centralne storitve e-podpisa s ključi imetnika (e-podpis, elektronski žig – electronic seal);
- uporabniški kriptografski ključ in digitalna potrdila;
- avtentikacija ob uporabi storitve, povezava s SI-CAS;
- registracija uporabnikov/potrdil (overitelj digitalnih potrdil, centralna storitev);
- aktiviranje uporabnikov/potrdil (generiranje ključev na centralnem strojnem varnostnem modulu HSM, prevzem digitalnih potrdil od overitelja digitalnih potrdil);
- upravljanje ključev (obnova, preklic, število ključev/potrdil na posameznega uporabnika);
- mehanizmi varovanja ključev (varna hramba zasebnih ključev, kriptografski mehanizmi varovanja zasebnih ključev);
- aktiviranje/de-aktiviranje uporabniških ključev ob uporabi storitve;
- tehnične značilnosti storitve (oblika podpisa, protokoli za dostop do storitve);
- varnostne zahteve (operativne varnostne zahteve, avtorizacija aktiviranja ključev storitve, beleženje dogodkov – audit);

Sledeča shema prikazuje konceptualni model sistema storitve centralnega strežniškega e-podpisa.



Slika 1 – Shematski model SI-CeS

2.1 Centralna storitev e-podpisa s ključi imetnika

Centralna storitev e-podpisa (SI-CeS) bo delovala kot zaledna storitev z naborom funkcij, potrebnih za kreiranje e-podpisa:

1. v okviru spletne aplikacije, na primer aplikacije v okviru spletnega poslovnega portala EKT oz. portala e-uprave ali
2. kreiranje e-podpisa na zahtevo uporabnika (ad-hoc e-podpis).

Oba načina sta opisana v nadaljevanju.

V primeru e-podpisa v okviru aplikacije spletnega portala bo podatek za e-podpis pripravila aplikacija ter ga vključila v zahtevek za e-podpis. Podatek za podpis bo lahko zgoščena vrednost (*hash*) dokumenta, dokument ali URL do podatkov za podpis. Zahtevek za e-podpis mora poleg podatka za e-podpis omogočati tudi posredovanje meta podatkov, kot je na primer tip zahtevanega e-podpisa. Tip zahtevanega e-podpisa opredeljuje zahtevani nivo e-podpisa, ki posredno opredeljuje potreben nivo SI-CAS avtentikacije, obliko e-podpisa (npr. XadES/SHA-1, PadES/SHA-256, CadES/SHA-1, raw/SHA-256 ...), ter po potrebi ostale parametre, ki bodo opredeljeni v tehničnih specifikacijah izdelani v okviru izvedbe. Aplikacija bo zahtevek za e-podpis posredovala SI-CeS ter hkrati preusmerila uporabnika na SI-CeS spletno stran. SI-CeS bo izvedel avtentikacijo uporabnika preko storitve SI-CAS, glede na zahtevani nivo e-podpisa, ter po uspešni avtentikaciji izvedel podpis zahtevka z uporabnikovim zasebnim ključem.

V primeru ad-hoc e-podpisa bo uporabnik preko spletne strani SI-CeS naložil dokument za podpis ter izbral tip e-podpisa. SI-CeS bo izvedel avtentikacijo uporabnika preko storitve SI-CAS glede na zahtevani tip e-podpisa. Po uspešni avtentikaciji bo izvedel podpis naloženega dokumenta. Po izvedenem podpisu bo uporabnik prenesel podpisani dokument. SI-CeS ne bo hranil niti kopij nepodpisanih niti kopij podpisanih dokumentov.

Funkcionalne zahteve so:

- Podpora za e-podpis na SI-CeS v okviru aplikacij spletnega portala (npr. aplikacija spletnega portala, ki potrebuje podpis, uporabnika skupaj preusmeri na centralni sistem SI-CeS, kjer se izvede e-podpisovanje).
- SI-CeS mora imeti aplikativni vmesnik oziroma spletno storitev (Web Service) za integracijo z aplikacijami spletnega portala.
- Vhodni podatek za e-podpis je lahko zgoščena vrednost (*hash*) dokumenta, dokument ali URL do podatkov za podpis.
- Dodatni vhodni parametri v zahtevku za e-podpis so v obliki meta podatkov oziroma oznake SI-CeS tipa e-podpisa.

- SI-CeS avtentikacija mora biti integrirana s SI-CAS (avtentikacija na SI-CeS se izvaja izključno preko SI-CAS, uporabnikovo identiteto določa SI-CAS identifikator, specifičen za SI-CeS).
- SI-CeS mora podpirati ad-hoc e-podpis posameznih dokumentov preko uporabniške spletne strani, ki mora omogočati nalaganje dokumenta za e-podpis in izbiro tipa e-podpisa ter preverjanje veljavnosti e-podpisa (glej razdelek 2.6.3).
- Omogočeno mora biti paketno podpisovanje, pri katerem uporabnik z enim vpisom uporabniškega gesla odobri podpis vseh dokumentov v paketu.
- Podpora za integratorje – za lažjo integracijo storitve v aplikacije spletnega portala se izdelava API za .NET in Java okolje.

Primer uporabe:

- Aplikacija spletnega portala, ki potrebuje e-podpis, izračuna zgoščeno vrednost dokumenta, ki ga uporabnik podpisujem ter uporabnika skupaj s tem podatkom in tipom podpisa preusmeri na SI-CeS.
- SI-CeS izvede avtentikacijo uporabnika preko SI-CAS.
- SI-CeS uporabniku prikaže podatke zahteve za podpis (npr. oznako aplikacije, ki je zahtevala podpis; namen podpisa in druge meta podatke, če so vsebovani v zahtevku), ter zahteva vnos uporabniškega gesla za izvedbo podpisa.
- SI-CeS iz svoje podatkovne baze v HSM naloži uporabnikov šifriran zasebni ključ, ga s pomočjo uporabniškega gesla in »HSM master« ključa dešifrira (dešifriranje se izvede v HSM) ter z njim na zahtevani način podpiše posredovano zgoščeno vrednost.
- SI-CeS pripravi odgovor v zahtevanem formatu (npr. XAdES), v katerega vključi podpis z uporabnikovim zasebnim ključem in pripadajoči javni ključ (digitalno potrdilo).
- SI-CeS podpiše celoten odgovor s svojim ključem ter ga z obvestilom o uspešnem podpisu in preusmeritvi vrne uporabniku.
- Uporabnik po pregledu statusa s klikom izvede preusmeritev na izhodiščno aplikacijo spletnega portala.

2.2 Uporabniški kriptografski ključi in digitalna potrdila

Digitalna potrdila overjajo zaupanja vredni overitelji digitalnih potrdil, kot so na primer overitelji kvalificiranih digitalnih potrdil, ali drugi splošno priznani javni overitelji digitalnih potrdil. V okviru SI-CeS je predvidena uporaba digitalnih potrdil Overitelja na Ministrstvu za notranje zadeve (MNZ), in sicer digitalnih potrdil za avtentikacijo (v povezavi s prijavo preko SMS OTP) ter digitalnih potrdil za elektronsko podpisovanje (za zagotavljanje nezatajljivosti oz. »non-repudiation«).

Trenutni model digitalnih potrdil je prilagojen hrambi in uporabi zasebnih kriptografskih ključev na strani uporabnika. Uporabnik pridobi od overitelja digitalno potrdilo pripadajočega javnega ključa z veljavnostjo do 5 let, kar mu omogoča uporabo zasebnega ključa v celotnem obdobju veljavnosti digitalnega potrdila. Isti model, to je veljavnost digitalnega potrdila do 5 let, kar je trenutna zakonska omejitev, je možno uporabiti tudi v primeru, ko se uporabniški ključi kreirajo, hranijo in uporabljajo na SI-CeS. Postopek registracije, kreiranja ključev in prevzema potrdila preko SI-CeS je opisan v poglavju »2.4 Upravljanje življenjskega cikla ključev in digitalnih potrdil imetnikov«. Zahteve za upravljanje uporabniških zasebnih ključev so opisane v poglavju »2.5 Varovanje zasebnih ključev imetnikov«.

V nadaljevanju so podane funkcionalne zahteve za sledeče primere uporabe digitalnih potrdil na SI-CeS:

- Imetnik pridobi digitalno potrdilo za avtentikacijo na osnovi registracije pri prijavi službi v skladu s pravili overitelja.
- Imetnik pridobi digitalno potrdilo za e-podpis na osnovi registracije z obstoječim digitalnim potrdilom.

2.2.1 Digitalno potrdilo za avtentikacijo

Imetnik pridobi digitalno potrdilo SI-CeS za avtentikacijo na osnovi registracijskega postopka v skladu s pravili overitelja:

- Registracija digitalnega potrdila pri overitelju (oddaja zahtevka in odobritev) se izvede v skladu s pravili delovanja overitelja.
- Uporabnik prevzame digitalno potrdilo preko spletne strani storitve SI-CeS. Avtentikacija zahtevka se izvede na osnovi aktivacijskih kod, ki jih je uporabnik prejel od overitelja (glej tudi poglavje »2.4 Upravljanje življenjskega cikla ključev in digitalnih potrdil imetnikov«) ter SI-CAS avtentikacije v povezavi z dvo-faktorsko identifikacijo na osnovi SMS OTP in uporabniškega gesla.
- Uporabnik v okviru postopka prevzema preko SI-CeS vpiše obstoječe SI-CAS geslo, ki ga bo poleg SMS OTP uporabljal kot uporabniško geslo za SI-CAS avtentikacijo s SI-CeS digitalnim potrdilom.
- V okviru postopka prevzema digitalnega potrdila se na sistemu SI-CeS generirajo uporabniški kriptografski ključi, ki se varno shranijo v bazi SI-CeS (glej poglavje »2.5 Varovanje zasebnih ključev imetnikov«). Zasebni ključ se šifrira s »HSM master ključem«, uporabniškim geslom in SI-CAS identifikatorjem. Digitalno potrdilo se shrani v SI-CeS bazo.

- Zasebni ključ uporabnika, kreiran na centralnem sistemu v okviru postopka prevzema se uporablja do izteka veljavnosti digitalnega potrdila oz. zasebnega ključa.

2.2.2 Digitalno potrdilo za e-podpis

V primeru, ko uporabnik že ima digitalno potrdilo enakega ali višjega nivoja zaupanja, kot ga bo prevzel preko sistema SI-CeS ter SI-CAS identiteto, lahko SI-CeS omogoči registracijo po elektronski poti. Imetnik pridobi digitalno potrdilo SI-CeS na osnovi obstoječega kvalificiranega digitalnega potrdila po sledečem postopku:

- SI-CeS na osnovi obstoječega veljavnega kvalificiranega digitalnega potrdila, s katerim se je uporabnik prijavil na SI-CAS, zahteva in izvede registracijo uporabnika pri overitelju (samodejna registracija, zahteve določi overitelj v svojih pravilih delovanja).
- Uporabnik v okviru postopka prevzema potrdila preko SI-CeS vpiše obstoječe SI-CAS geslo, ki ga bo poleg SI-CAS identitete uporabljal kot uporabniško geslo za kreiranje e-podpisa preko SI-CeS.
- Po uspešni registraciji se v okviru postopka prevzema digitalnega potrdila na sistemu SI-CeS generirajo uporabniški kriptografski ključ, ki se varno shranijo v bazi SI-CeS (glej tudi »2.5 Varovanje zasebnih ključev imetnikov«). Zasebni ključ se šifrira s »HSM master ključem«, uporabniškim geslom in SI-CAS identifikatorjem. Digitalno potrdilo se shrani v SI-CeS bazo.
- Zasebni podpisni ključ uporabnika, kreiran na centralnem sistemu v okviru postopka prevzema, se uporablja do izteka veljavnosti pripadajočega digitalnega potrdila oz. zasebnega ključa.
- Po uspešnem prevzemu potrdila za podpis se uporabnika o tem obvesti po e-pošti.

2.2.3 Dodatne zahteve

Dodatne funkcionalne zahteve:

- V digitalnih potrdilih ni elektronskega poštnega naslova, a se ta podatek vseeno hrani v podatkovni bazi sistema SI-CeS (opcija: sistema SMS OTP v primeru digitalnih potrdil za avtentikacijo) za potrebe obveščanja o poteku veljavnosti digitalnih potrdil.
- Pri avtentikaciji uporabnika SI-CAS posreduje SI-CeS le SI-CAS identifikator, specifičen za uporabo v okviru SI-CeS sistema, ter v primeru registracije uporabnika tudi druge potrebne attribute (npr. ime in priimek).
- [Dodatna možnost]. Digitalno potrdilo vsebuje SI-CAS identifikator v zasebnem (»custom«) polju v skladu s specifikacijo X.509, ali v DN polju (»SerialNumber«, ali »Pseudonym«).

- Kot ključ za iskanje uporabnikovega zasebnega ključa v podatkovni bazi se uporabljata:
 - zgoščena vrednost, izračunana iz SI-CAS identifikatorja in uporabniškega gesla; ali
 - zgoščena vrednost šifriranega digitalnega potrdila.

Dodatna ne-funkcionalna zahteva:

- Vsak uporabnik poseduje največ eno digitalno potrdilo za vsak nivo e-podpisa, ki ga omogoča SI-CeS.

2.3 Avtentikacija ob uporabi storitve SI-CeS

Avtentikacija uporabnikov ob dostopu do storitve SI-CeS se bo izvajala na Centralnem avtentikacijskem sistemu (SI-CAS). Za opis SI-CAS glej dokument »[EKT2-CAS]-Funkcionalne specifikacije in tehnična zasnova_v1.1.pdf«.

SI-CAS bo omogočal prijavo z e-identitetami različnih nivojev zaupanja, od najnižjega nivoja (uporabniška imena in gesla, Facebook profil, Google profil, ...) do najvišjih nivojev (e-identiteta na varnem mediju, npr. na pametni kartici), ki jih bodo zagotovili različni ponudniki identitet. Zaupanje v identiteto uporabnika je ključnega pomena pri uporabi centralnega e-podpisa, zato mora biti omogočena kontrola nivoja SI-CAS avtentikacije in omejitev uporabe, oziroma kreiranja e-podpisa različnih nivojev zaupanja glede na nivo SI-CAS avtentikacije.

Funkcionalne zahteve so:

- Avtentikacija uporabnikov storitve SI-CeS se izvaja izključno preko SI-CAS.
- Za avtentikacijo preko SI-CAS se uporablja protokol SAML verzije 2. Dovoljena je uporaba enkratne prijave (angl. Single Sign-On, SSO) v okviru SI-CAS, vendar mora SI-CeS zahtevati uporabniško geslo za podpis ob vsakem zahtevku za e-podpis, tudi v primeru, če je uporabnik že prijavljen na SI-CAS preko druge aplikacije (uporaba enkratne prijave).
- Podprto mora biti razločevanje nivojev SI-CAS avtentikacije, kot so oz. bodo določeni v okviru pravil delovanja SI-CAS.
- SI-CeS mora zahtevati enak ali višji nivo SI-CAS avtentikacije, kot je potreben glede na tip e-podpisa v zahtevku za podpis.

2.3.1 Nivoji SI-CAS avtentikacije in e-podpisa

Podprti morajo biti vsaj sledeči nivoji e-podpisa glede na nivo SI-CAS avtentikacije³:

Nivo e-podpisa	Zahtevani nivo SI-CAS avtentikacije
Kvalificiran elektronski podpis	Višji nivo
Napreden elektronski podpis overjen s kvalificiranim digitalnim potrdilom	Srednji nivo
Napreden elektronski podpis	Nižji nivo

Tabela 1 – Zahtevan (minimalni) nivo SI-CAS avtentikacije glede na nivo e-podpisa

Nivoji e-podpisa SI-CeS so usklajeni z zahtevami in definicijami e-podpisa v Zakonu o elektronskem poslovanju in elektronskem podpisu (v nadaljevanju ZEPEP), Uredbi in EU Direktivi 1999/93/EC za e-podpis (v nadaljevanju Direktiva). V nadaljevanju poglavja je podan opis nivojev e-podpisa SI-CeS ter dodaten opis ključnih pojmov.

Nivoji e-podpisa SI-CeS:

- **Kvalificiran elektronski podpis** – Napreden elektronski podpis overjen s kvalificiranim digitalnim potrdilom in oblikovan z varno napravo za podpisovanje, ki izpolnjuje zahteve za sredstva za varno elektronsko podpisovanje (v nadaljevanju SSCD). E-podpis se uporablja v skladu z ZEPEP, 15. člen.
- **Napreden elektronski podpis overjen s kvalificiranim digitalnim potrdilom** – Napreden elektronski podpis overjen s kvalificiranim digitalnim potrdilom. E-podpis se uporablja v skladu z ZEPEP, 14. člen.
- **Napreden elektronski podpis** – Napreden elektronski podpis overjen z normaliziranim (standardnim) digitalnim potrdilom. E-podpis se uporablja v skladu z ZEPEP, 14. člen.

Opis ključnih pojmov nivojev e-podpisa SI-CeS (glej tudi Direktivo):

- **Kvalificirano digitalno potrdilo (QC)** – Potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto, ki izpolnjuje zahteve iz Direktive Annex I in ki ga izda overitelj, deluje v skladu z zahtevami iz Direktive Annex II.

³ V času priprave dokumenta nivoji SI-CAS še niso definirani.

- **Normalizirano (standardno) digitalno potrdilo** – Potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto, ki ga je izdal splošno priznani overitelj (SI-CeS potrjeni overitelj).
- **SI-CeS priznani (potrjeni) overitelji** – Nabor overiteljev, ki so priznani na nivoju storitve SI-CeS. Kriterij za vključitev overiteljev na seznam SI-CeS priznanih overiteljev je, da je overitelj registriran v okviru Microsoft ali Mozilla Root CA programa, ali na drug način, skladno s pravili delovanja SI-CeS, izkaže nivo zaupanja v digitalna potrdila, ki jih izdaja.
- **Napreden elektronski podpis** – glej definicijo »advanced electronic signature« v 2. členu Direktive.
- **Varna naprava za podpisovanje (SSCD)** – glej definicijo »secure-signature-creation device« v 2. členu Direktive.

Funkcionalne zahteve so:

- SI-CeS mora omogočati nivoje podpisa navedene v Tabeli 1.
- Pri kreiranju podpisa mora biti uporabljeno digitalno potrdilo SI-CeS minimalno nivoja kot je določeno v zahtevku.
- Pri kreiranju podpisa je dovoljena uporaba digitalnega potrdila SI-CeS višjega nivoja, če uporabnik nima digitalnega potrdila zahtevanega nivoja, ima pa višjega.
- Dovoljena je uporaba SI-CAS avtentikacije višjega nivoja, kot je zahtevan, če uporabnik pri avtentikaciji izbere SI-CAS avtentikacijo višjega nivoja.

2.4 Upravljanje življenjskega cikla ključev in digitalnih potrdil imetnikov

Sistem SI-CeS bo imel v postopkih prevzema digitalnih potrdil funkcijo vmesnika med uporabniki in overiteljem. Vsi postopki v povezavi z upravljanjem digitalnih potrdil, kot so registracija uporabnikov, odobritev in procesiranje zahtevkov za izdajo, obnovo, preklic, ..., bodo še naprej v pristojnosti overitelja in jih bo izvajal overitelj. Sistem SI-CeS mora za potrebe upravljanja življenjskega cikla ključev in digitalnih potrdil imetnikov zagotoviti potrebne funkcije za generiranje kriptografskih ključev na HSM, generiranje zahtevkov za overjanje digitalnih potrdil (npr. PKCS#10, ali z uporabo CMP), varno hrambo zasebnih ključev imetnikov ter interno evidenco digitalnih potrdil imetnikov.

V primeru, ko imetnik pridobi digitalno potrdilo na SI-CeS na osnovi obstoječega kvalificiranega digitalnega potrdila, se celoten postopek registracije digitalnega potrdila pri overitelju in prevzema izvede preko SI-CeS (glej poglavje 2.2).

2.4.1 Upravljanje digitalnih potrdil za avtentikacijo

2.4.1.1 Registracija uporabnikov

Opis registracije uporabnikov in aktiviranje digitalnih potrdil na SI-CeS je podan v poglavju »2.2 Uporabniški kriptografski ključi in digitalna potrdila«.

Po oddaji zahtevka in uspešni registraciji na prijavnih službi overitelja, uporabnik v skladu s pravili overitelja prejme aktivacijske kode, ki jih potrebuje za prevzem digitalnega potrdila za avtentikacijo.

2.4.1.2 Prva aktivacija uporabnikov in potrdil na SI-CeS

Po prejemu aktivacijskih kod, uporabnik izvede aktiviranje in prevzem digitalnega potrdila za avtentikacijo. Podatke za prevzem (aktivacijske kode, uporabniško geslo za odobritev podpisa na SI-CeS) uporabnik vnese na začetku postopka. SI-CeS vrne potrditev izvedbe prevzema in možnost prenosa izdanega digitalnega potrdila k uporabniku. Glej razdelek 2.2.1.

2.4.1.3 Obnova potrdila

Obnova digitalnega potrdila za avtentikacijo se izvede pred potekom obdobja veljavnosti trenutnega digitalnega potrdila. Pogoje za obnovo prepíše overitelj v svojih pravilih delovanja.

Obnova digitalnega potrdila za avtentikacijo se izvede on-line in mora biti izvedena v skladu s sledečimi funkcionalnimi zahtevami oz. postopkom:

- Uporabnik se po prejemu obvestila o bližajočem se poteku obdobja veljavnosti trenutnega digitalnega potrdila preko spletne aplikacije prijavi z veljavno SI-CAS avtentikacijo na osnovi digitalnega potrdila ustreznega nivoja v skladu s pravili overitelja.
- SI-CeS izvede obnovo potrdila, generira se nov par ključev, zasebni ključ se šifrira s HSM master ključem, uporabniškim geslom in SI-CAS identifikatorjem ter shrani v bazo.

Iz baze se briše zapis za šifriran zasebni ključ, ki se nanaša na prejšnje potrdilo.

2.4.1.4 Upravljanje uporabnikov sistema SI-CeS

Upravljanje uporabnikov obsega funkcije potrebne za upravljanje uporabniškega računa na sistemu SI-CeS, in sicer:

- Sprememba uporabniškega gesla za zaščito zasebnega ključa se izvede v okviru spremembe gesla na SI-CAS. Glej tudi razdelek 2.4.1.4.1.
- Ponastavitev pozabljenega uporabniškega gesla ni možna.

- Ukinitve uporabniškega računa na SI-CeS se izvede kot brisanje pripadajočih zasebnih ključev iz aktivne baze SI-CeS. Glej tudi razdelek 2.4.2.4.2.
- Preklic digitalnega potrdila prevzetega preko SI-CeS

2.4.1.4.1 Sprememba uporabniškega gesla

Sprememba uporabniškega gesla mora biti izvedena v skladu s sledečimi funkcionalnimi zahtevami oz. postopkom:

- Uporabnik se na SI-CeS prijavi preko SI-CAS avtentikacije, določi novo geslo in transakcijo podpiše z obstoječim digitalnim potrdilom za e-podpis na SI-CeS.
- Za vsako aktivno digitalno potrdilo⁴ SI-CeS naloži v HSM pripadajoč šifriran uporabnikov zasebni ključ.
- Uporabnikov zasebni ključ se v HSM dešifrira z uporabo starega uporabniškega gesla.
- Po dešifriranju se zasebni ključ ponovno šifrira v HSM z uporabo novega uporabniškega gesla in shrani v bazo SI-CeS.
- Kopija zasebnega ključa, zaščitena s starim uporabniškim geslom, se varno briše iz aktivne baze.

2.4.1.4.2 Ponastavitev pozabljenega uporabniškega gesla

Ponastavitev pozabljenega uporabniškega gesla ni možna. Če uporabnik pozabi uporabniško geslo, se izvede deaktiviranje obstoječih aktivnih digitalnih potrdil. Deaktiviranje se izvede kot varno brisanje kopij pripadajočih zasebnih ključev iz aktivne baze SI-CeS. Novo digitalno potrdilo za avtentikacijo lahko uporabnik pridobi v skladu s pravili overitelja, tako kot ob prvi izdaji. Novo potrdilo za e-podpis se generira ob prvi naslednji uporabi podpisa, tako kot ob prvi izdaji.

2.4.1.4.3 Ukinitve (odjava) storitve

Uporabnik lahko izvede postopke ukinitve (odjave) storitve, ko ne želi več uporabljati storitve oz. po svoji presoji. Odjava storitve na SI-CeS nima za posledico preklic njegovega digitalnega potrdila. V primeru, da želi tudi preklicati potrdilo, mora oddati zahtevek za preklic v skladu s pravili delovanja overitelja.

Odjava storitve mora biti izvedena v skladu s sledečimi funkcionalnimi zahtevami, oziroma postopkom:

- Uporabnik se preko spletne strani in z uporabo SI-CAS avtentikacije prijavi na SI-CeS.
- Odda zahtevek za odjavo in zahtevek podpiše.
- SI-CeS izbriše iz aktivne baze kopijo šifriranega zasebnega ključa.

⁴ Uporabnik ima lahko eno potrdilo za avtentikacijo in eno ali več potrdil za e-podpis.

- [Dodatna možnost]. Uporabnik lahko hkrati odda podpisan zahtevek za preklic digitalnega potrdila. Omejitev – možnost mora podpirati tudi overitelj.

2.4.1.4.4 Preklic digitalnega potrdila

Preklic potrdila na SI-CeS se izvede v primeru razkritja uporabniškega gesla in drugih primerih, ki so določeni v pravilih overitelja. Obnova digitalnega potrdila za avtentikacijo po preklicu se izvede kot postopek prvega prevzema.

2.4.2 Upravljanje digitalnih potrdil za digitalni podpis

2.4.2.1 Registracija uporabnikov

Opis registracije uporabnikov in aktiviranje digitalnih potrdil na SI-CeS je podan v poglavju »2.2 Uporabniški kriptografski ključi in digitalna potrdila«.

Ob prvem zahtevku za podpis se bodoči imetnik preko spletne aplikacije prijavi s SI-CAS prijavnim sredstvom ustreznega nivoja (npr. za nivo 3 je potrebna prijava s kvalificiranim digitalnim potrdilom). Postopek registracije digitalnega potrdila in aktiviranje se izvede, kot je opisano v razdelku 2.2.2 za primer, ko uporabnik pridobi potrdilo SI-CeS na osnovi obstoječega kvalificiranega digitalnega potrdila.

2.4.2.2 Prva aktivacija uporabnikov in potrdil na SI-CeS

Aktivacija digitalnega potrdila za podpis se izvede ob prvem zahtevku za podpis (glej tudi razdelek 2.2.2), neposredno po uspešni registraciji uporabnika.

Zahteve v povezavi z overiteljem:

- SI-CeS mora imeti možnost kontrole prevzema ustreznega potrdila. Na primer, nadzor da uporabnik ne prevzame SIGEN-CA potrdila, ki je bilo sicer registrirano kot spletno potrdilo in ne SI-CeS potrdilo.

2.4.2.3 Obnova potrdila

Obnova digitalnega potrdila za podpis se izvede ob prvi uporabi podpisa po poteku potrdila, po postopku kot se izvede ob prvi izdaji.

[Dodatna možnost]. Obnova se izvede v določenem obdobju pred iztekom veljavnosti (npr. 30% veljavnosti), če uporabnik v tem obdobju izvede podpis. *Komentar: tako se izognemo primeru, da nekdo podpiše s potrdilom tik pred iztekom veljavnosti in je podpis praktično takoj "potekel".*

2.4.2.4 Upravljanje uporabnikov sistema SI-CeS

Kot pri digitalnih potrdilih za avtentikacijo (glej razdelek 2.4.1.4).

2.4.2.4.1 Sprememba uporabniškega gesla

Kot pri digitalnih potrdilih za avtentikacijo (glej razdelek 2.4.1.4.1).

2.4.2.4.2 Ponastavitev pozabljenega uporabniškega gesla

Kot pri digitalnih potrdilih za avtentikacijo (glej razdelek 2.4.1.4.2).

2.4.2.4.3 Ukinitev (odjava) storitve

Kot pri digitalnih potrdilih za avtentikacijo (glej razdelek 2.4.1.4.3).

2.4.2.4.4 Preklic digitalnega potrdila

Preklic potrdila na SI-CeS se izvede v primeru razkritja uporabniškega gesla in v drugih primerih, določenih v pravilih overitelja. Obnova digitalnega potrdila za digitalni podpis po preklicu ni potrebna. Izdaja novega potrdila se izvede ob prvem zahtevku za e-podpis.

2.4.3 Dodatni vidiki upravljanja digitalnih potrdil in uporabniških ključev

Preklic potrdil se izvaja le ob nevarnosti zlorabe (na primer razkritja uporabniškega gesla). V drugih primerih, kot so obnova, potek veljavnosti, ..., se iz baze briše le pripadajoči šifriran zasebni ključ.

Upravljanje varnostnih kopij mora biti izvedeno na osnovi sledečih zahtev:

- Vsaka varnostna kopija je šifrirana s svojim ključem, ki je shranjen na HSM. Hranijo se samo kopije zadnjih treh (ali kot se določi v politiki) ključev za šifriranje varnostnih kopij. Starejši ključi se brišejo iz HSM po uspešni izdelavi zadnje varnostne kopije.
- Za namestitev varnostne kopije je potrebna večkratna avtorizacija upravljavcev sistema po principu »multi-person-control« (npr. 2/3 avtorizacija za uporabo dešifrirnega ključa na HSM ali principu »split-knowledge«).
- Varnostno kopiranje se izvaja po vsakem preklicu (ali: vsaj enkrat dnevno, enkrat na uro oz. kot je določeno v pravilih overitelja).

2.5 Varovanje zasebnih ključev imetnikov

2.5.1 Varna hramba zasebnih ključev

SI-CeS mora zagotoviti varno hrambo uporabniških zasebnih ključev. Varna hramba uporabniških zasebnih ključev mora biti izvedena na osnovi sledečih zahtev:

- Vse operacije s kriptografskimi ključi se morajo izvajati na strojnih kriptografskih modulih (HSM), tako da se ključi nikdar ne pojavijo izven HSM v nešifrirani obliki.
- Uporabniški ključi morajo biti varovani na način, da jih ni možno uporabiti brez uspešne avtentikacije uporabnika.
- Uporabniški avtentikacijski podatki (uporabniško geslo) ne smejo biti shranjeni na sistemu SI-CeS.
- Vnos uporabniških avtentikacijskih podatkov mora biti izveden preko verodostojne komunikacijske poti.
- Vsa izmenjava podatkov in vse komunikacije znotraj sistema SI-CeS morajo biti izvedene preko varnih komunikacijskih kanalov.
- Sistemski administratorji SI-CeS in HSM ne smejo imeti dostopa do uporabniških ključev na način, ki bi omogočal kreiranje e-podpisa.
- Administratorski dostopi morajo biti izvedeni z uporabo principa »Dual Control« ali »Split Knowledge«.

V okviru rešitve je potrebno izdelati »SSCD Protection Profile« specifikacije za centralno storitev e-podpisa.

2.5.2 Aktiviranje/de-aktiviranje uporabniških ključev ob uporabi storitve

Aktiviranje uporabniških zasebnih ključev je dovoljeno samo po uspešni avtentikaciji uporabnika na SI-CAS in ob vpisu veljavnega uporabniškega gesla. Po uspešni identifikaciji se naložijo šifrirane kopije uporabniških ključev v HSM, iz uporabniškega gesla, SI-CAS identifikatorja in master ključa se na HSM generira dešifrirni ključ, ki se uporabi za dešifriranje uporabniških ključev znotraj HSM. Po končani uporabi (izvedenem podpisu), se kopije uporabniških ključev v HSM varno uničijo. Kopije uporabniških ključev ne smejo nikdar ostati na HSM ali se izvoziti iz HSM v »berljivi« obliki oz. obliki, ki bi omogočila uporabo ključev brez odobritve uporabnika.

2.6 Tehnične zahteve e-podpisa

V poglavju so podane zahteve za oblike e-podpisa, ki jih mora podpirati SI-CeS.

Posamezna oblika podpisa, ki jo lahko zahteva uporabnik storitve, mora biti opisana v obliki profila, ki opisuje vse potrebne lastnosti za kreiranje podpisa. Na primer format (raw, XAdES, ...), algoritem (SHA-1, SHA-256, ...), oblika vhodnih podatkov, ...

2.6.1 Oblike vhodnih podatkov za podpis

Podatki za podpis se lahko posreduje kot:

- Zgoščena (hash) vrednost dokumenta (vsaj SHA-1, SHA-256)
- Dokument v izvorni obliki
- URL do spletne strani ali dokumenta

2.6.2 Oblike e-podpisa SI-CeS

SI-CeS mora podpirati sledeče formate e-podpisa⁵:

- XMLDSig
 - W3C Recommendation 10 June 2008
<http://www.w3.org/TR/2008/REC-xmlsig-core-20080610/>
- XAdES (B-Level, T-Level, TL-Level, LTA-Level) v skladu s specifikacijami:
 - ETSI TS 103 171
http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf
 - ETSI TS 101 903
http://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.02_60/ts_101903v010402p.pdf

⁵ Zahteve glede podprtih formatov naprednega (AdES) e-podpisa so določene v Odločbi Evropske komisije 2011/130/EU o minimalnih zahtevah za čezmejno obravnavo e-podpisanih dokumentov s strani pristojnih institucij po storitveni direktivi (Ur. l. Evropske unije, L 53/54).

- PAdES (B-Level, T-Level, TL-Level, LTA-Level)
 - ETSI TS 103 172
http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.01.01_60/ts_103172v020101p.pdf
 - ETSI TS 102 778-3
http://www.etsi.org/deliver/etsi_ts/102700_102799/10277803/01.02.01_60/ts_10277803v010201p.pdf
 - ETSI TS 102 778-4
http://www.etsi.org/deliver/etsi_ts/102700_102799/10277804/01.01.02_60/ts_10277804v010102p.pdf
- CAdES
 - ETSI TS 101 733 CAdES
http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.01.01_60/ts_101733v020101p.pdf
- 'raw' format podpisa (PKCS#1 'raw RSA')

Podpora za formate e-podpisa mora biti izvedena na način, ki omogoča naknadno spreminjanje podprtih formatov in dopolnjevanje njihovega nabora skladno z morebitnimi spremembami tehničnih priporočil in pravnih aktov.

2.6.3 Preverjanje veljavnosti e-podpisa

V okviru storitve SI-CeS mora biti vzpostavljen tudi mehanizem za preverjanje veljavnosti oblik e-podpisov, navedenih v razdelku »2.6.2. Storitve preverjanja veljavnosti digitalnega podpisa«. Vzpostavljen mora biti kot samostojni modul, ki bo kot centralna storitev na voljo tudi drugim informacijskim sistemom, oz. rešitvam. Storitev bo predvidoma uporabljala odprto-kodno rešitev Evropske komisije (DSS⁶).

2.6.4 Dodatne storitve

SI-CeS mora podpirati sledeče dodatne storitve e-podpisa:

- Časovni žig (Timestamp) v skladu z RFC 3161
- OCSP – preverjanje veljavnosti digitalnega potrdila

Odjemalec lahko v okviru zahtevka za e-podpis zahteva tudi časovni žig in/ali OCSP status. V tem primeru mora SI-CeS poslati ustrezne zahtevke na sistem za časovno žigosanje oziroma sistem za sprotne preverjanje veljavnosti digitalnih potrdil ter časovni žig in/ali OCSP status vključiti v e-podpis oz. odgovor odjemalcu.

⁶ <https://joinup.ec.europa.eu/software/sd-dss/release/all>

2.7 Operativne in varnostne zahteve

2.7.1 Aktiviranje kriptografskih ključev

Aktiviranje ključev SI-CeS na strojnem varnostnem modulu (HSM) mora biti po principu »multi-person-control« (npr. 2/3 avtorizacija ali »split-knowledge«).

2.7.2 Strojni varnostni moduli (HSM)

Strojni varnostni moduli morajo imeti potrdilo o skladnosti s FIPS 140-2 Level 3 (ali višjim) ali EAL4+ (ali višjim).

2.7.3 Zahteve za beleženje

Vsi dogodki z uporabniškimi ključi morajo biti zabeleženi v obliki varne revizijske sledi, ki mora biti zaščitena pred neopaznimi spremembami.

Ostali dogodki morajo biti zabeleženi v operativni beležki, ki ne sme vsebovati varnostno občutljivih podatkov.

Dodatek – kratice in pojmi

Kratice

- AN SREP – Akcijski načrto e-poslovanja javne uprave
- CMP – Certificate Management Protokol
- EKT – Enotna kontaktna točka
- HSM – strojni varnostni modul (angl. Hardware Security Module)
- SI-CAS – Centralni avtentikacijski sistem
- SI-CeS – Centralni (strežniški) e-podpis
- SMS OTP – enkratno geslo prejeto v kratkem tekstovnem sporočilu
(angl. One Time Password sent over Short Message Service)
- SSCD – Sredstvo za varno elektronsko podpisovanje
(angl. Secure Signature Creation Device)
- ZEPEP – Zakon o elektronskem poslovanju in elektronskem podpisu

Pojmi

- **SI-CAS identifikator** je oznaka, ki jo SI-CAS dodeli subjektu in je specifična za uporabo v okviru SI-CeS.
- **SI-CAS identiteta** predstavlja nabor podatkov, ki enolično opisuje določen subjekt.
- **SI-CAS prijavno sredstvo** je identifikacijski mehanizem, ki ga je uporabnik registriral na SI-CAS.
- **SI-CAS avtentikacija** je prijava v storitev preko SI-CAS sistema.
- **HSM master ključ** je kriptografski ključ, generiran in shranjen na HSM, ki se uporablja kot glavni ključ za šifriranje uporabniških ključev.