Politika potpisivanja Službenog lista

Verzija 4

(1.3.171.4.1.1.4)

Primjenjuje se od 1. listopada 2023.

Sadržaj

1. Uvod

U ovom se dokumentu utvrđuje politika potpisivanja Službenog lista Europske unije (potpisivanje SL-a) i pečaćenja Službenog lista (pečaćenje SL-a), koji služe za dokazivanje vjerodostojnosti elektroničke verzije Službenog lista Europske unije (SL) u skladu s Uredbom Vijeća (EU) br. 216/2013 o elektroničkom izdanju Službenog lista Europske unije[1].

Politika potpisivanja skup je pravila za stvaranje, provjeravanje valjanosti i dopunjavanje jednog ili više međusobno povezanih elektroničkih potpisa i/ili pečata kojima se definiraju tehnički i proceduralni zahtjevi za njihovo stvaranje, provjeru njihove valjanosti i dugoročno upravljanje njima kako bi se zadovoljile posebne poslovne potrebe i odredilo kad su oni važeći. Svrha je politike potpisivanja učiniti sve aspekte određenog postupka potpisivanja ili pečaćenja jasnima svim zainteresiranim stranama, tj. potpisnicima, primateljima i arbitrima, tako da elektronički potpisi i pečati koji ispunjavaju zahtjeve politike mogu povećati povjerenje u primjenjivost i prihvatljivost tih potpisa i pečata.

Detaljni nacrti politike potpisivanja objašnjeni su u dokumentu [ETSI 2015.], u kojem se definiraju i smjernice i struktura ovog dokumenta. Ključne riječi „MORA”, „NE SMIJE”, „OBAVEZNO”, „JEST”, „NIJE”, „TREBALO BI”, „NE BI TREBALO”, „PREPORUČENO”, „MOŽE” i „NEOBAVEZNO” u ovom dokumentu trebaju se tumačiti u skladu s opisom u normi RFC 2911 [Bradner 1997.].

SL služi kao jedini vjerodostojni izvor prava EU-a, a objavljuje ga Ured za publikacije Europske unije (OP) na internetskim stranicama EUR-Lex (vidjeti 1.2.4.). SL se objavljuje od ponedjeljka do petka, te ponekad vikendom, na svim službenim jezicima Europske unije (EU). *U daljnjem se tekstu skraćenica „SL” upotrebljava za zajedničko označavanje ovog posebnog područja primjene.*

1.1. Pregled

Politikom potpisivanja SL-a oblikuju se ključni elementi izrade elektroničkog potpisa i elektroničkog pečata, provjere valjanosti i dugoročnog čuvanja kada se primjenjuje na SL kao način dokazivanja vjerodostojnosti izdanja SL-a koja objavljuje OP.
Sastoji se od:

- uvoda, koji obuhvaća naziv/oznaku politike, detalje o izdavaču politike, administraciju politike, definicije i skraćenice itd.,
- izjava o praksama u vezi s aplikacijama za potpisivanje, kojima se definiraju pripadajuća politika i pravni zahtjevi, kao i primjenjive sigurnosne napomene,
- parametara za utvrđivanje opsega djelovanja, kojima se detaljno opisuju postupci izrade elektroničkih potpisa i pečata kojima se dokazuje vjerodostojnost izdanja SL-a koja objavljuje OP,
- zahtjevâ i izjava o provedbi tehničkih mehanizama i normi, te prilogâ.

1.2. Područje djelovanja

1.2.1. Područje primjene i ograničenja politike potpisivanja

Politika potpisivanja SL-a obuhvaća elektroničke potpise i pečate koje za pojedina izdanja SL-a izrađuju ovlašteni potpisnici SL-a u skladu s Uredbom Vijeća o elektroničkom izdanju

[1] Vidjeti SL L 69, 13.3.2013., str. 1.

Službenog lista Europske unije nakon uspješne provjere valjanosti svakog izdanja koje se potpisuje.

1.2.2. Područje primjena

Elektronički potpisi i pečati obuhvaćeni politikom potpisivanja SL-a samo su oni opisani u odjeljku 3.1.

1.2.3. Transakcijski kontekst

Nije primjenjivo.

1.3. Pravila o nazivu, identifikaciji i usklađenosti politike potpisivanja

1.3.1. Naziv politike

Politika potpisivanja SL-a nosi sljedeći naziv:

Politika potpisivanja Službenog lista

1.3.2. Identifikator politike

Budući da postoji samo jedan Službeni list Europske unije i da je njegovo objavljivanje dobro poznat postupak Europske unije, politiku potpisivanja SL-a može implicitno identificirati bilo koja strana. Opis općeg tijeka rada naveden je u odjeljku 3.1.1.1.

Kako bi se eksplicitno označila politika, svaki potpis i pečat SL-a *MOŽE* uključivati eksplicitnu oznaku politike potpisivanja definiranu u odjeljku 5.2.9. [ETSI 2022-XAdES]. Ako je prisutna, eksplicitna oznaka politike potpisivanja OZNAČAVA identifikator objekta (OID) 1.3.171.4.1.1.4. primjenjujući pravila za kodiranje utvrđena u odjeljku 5.2.9. u [ETSI 2022-XAdES] i [Mealling 2010.].

Globalni jedinstveni identifikator objekta 1.3.171.4.1.1.4. nedvosmisleno identificira sadašnju verziju te politike. Prefiks 1.3.171.4. prijavljen je kao osnovni OID za *Politike potpisivanja i druge svrhe Ureda za publikacije EU-a* (vidjeti http://www.oid-info.com/get/1.3.171.4). Sufiks 1.1.4. označava sadašnju verziju politike potpisivanja SL-a, a njezina oznaka vrijednosti ASN.1 GLASI {sl(1) politika-potpisivanja(1) verzija(4)}. Od ove verzije politike verzija 1.1.3. prestaje važiti.

1.3.3. Pravila usklađenosti politike

Za ovu se politiku ne jamči da je usklađena s bilo kojom drugom politikom.

1.3.4. Distribucijske točke politike

Dokument politike potpisivanja SL-a objavljen je na internetskim stranicama EUR-Lex. Dostupan je na internetskim stranicama Ureda za publikacije: https://eur-lex.europa.eu/.

1.3.5. Razdoblje važenja politike

Ova verzija politike na snazi je od 1. listopada 2023.

1.3.6. Područje primjene politike

Ova politika primjenjuje se na sva izdanja SL-a koja su objavljena i elektronički potpisana nakon stupanja na snagu Uredbe Vijeća o elektroničkom izdanju Službenog lista Europske unije. Ne primjenjuje se na Dodatak Službenom listu Europske unije (serije S, Službeni list S ili SL S).

NAPOMENA: Svaka verzija ove politike valjana je u razdoblju važenja utvrđenom u svakoj verziji. Skup svih verzija obuhvaća sva izdanja SL-a.

1.4. Upravljanje dokumentima politike potpisivanja

Izdavač politike potpisivanja SL-a jest Ured za publikacije Europske unije, koji donosi ovaj dokument i objavljuje ga na internetskim stranicama EUR-Lex.

Politika potpisivanja SL-a u obliku u kojem je objavljena automatski IMA pravnu snagu i PRIMJENJUJE SE na izradu i provjeru potpisa i pečata SL-a i dugoročno upravljanje njima.

Izdavač politike potpisivanja SL-a odgovoran je za:

- utvrđivanje i odobravanje politike potpisivanja SL-a,
- definiranje postupka pregleda za politiku potpisivanja SL-a,
- definiranje kriterijâ ocjenjivanja i postupka kojima se osigurava da je politika potpisivanja SL-a u skladu s Uredbom Vijeća (EU) br. 216/2013 od 7. ožujka 2013. o elektroničkom izdanju Službenog lista Europske unije i Uredbom Vijeća (EU) 2018/2056 od 6. prosinca 2018. o izmjeni Uredbe (EU) br. 216/2013 o elektroničkom izdanju Službenog lista Europske unije,
- definiranje kriterijâ ocjenjivanja i postupka kojima se osigurava da su sve aplikacije za koje se tvrdi da su usklađene s politikom potpisivanja SL-a doista usklađene s njezinim trenutačno važećim pravilima,
- objavljivanje politike potpisivanja SL-a i njezinih izmijenjenih verzija na stranicama EUR-Lex.

1.4.1. Nadležno tijelo za politiku

Politikom potpisivanja SL-a upravlja Ured za publikacije Europske unije.

1.4.2. Osoba za kontakt

Izdavaču ove politike možete se obratiti koristeći se sljedećim podacima:

Osoba za kontakt:	Načelnik odjela za Službeni list i sudsku praksu
Poštanska adresa:	2, rue Mercier, L-2985 Luxembourg
Telefonski broj:	+352 29291
Broj telefaksa:	+352 292944620
E-adresa:	OP-JO-AUTHENTIQUE-HELPDESK@publications.europa.eu

1.4.3. Postupak odobravanja

Glavni direktor Ureda za publikacije Europske unije je nadležno tijelo za odobravanje politike u Uredu za publikacije Europske unije.

1.4.4. Verzije politike

Početne i izmijenjene verzije politike *MOGU* sadržavati najraniji datum stupanja na snagu. Kada se neka verzija politike objavi, STUPA na snagu najkasnije na jedan od sljedećih triju datuma:

1. najraniji datum stupanja na snagu ako je naveden u toj verziji politike;
2. dan nakon najranijeg datuma vremenskog žiga potpisa na potpisu ili pečatu SL-a u izdanju SL-a u kojemu se navodi verzija politike koja se objavljuje, prema lokalnom vremenu u Luksemburgu;
3. dan nakon datuma objavljivanja te verzije politike.

Svaka izmijenjena verzija politike automatski PRESTAJE važiti nakon stupanja na snagu sljedeće izmijenjene verzije. U sljedećoj izmijenjenoj verziji politike TREBA navesti i naziv prethodne verzije koja prestaje važiti.

Prethodno navedena pravila osmišljena su kako bi se osiguralo da potpisivanje bilo koje verzije politike ne bude podložno, izravno ili neizravno, istoj verziji politike kako bi se spriječilo kružno zaključivanje. Uz to, preporučuje se zadržati verziju koja prestaje važiti.

1.5. Definicije i kratice

Definicije i kratice koji se upotrebljavaju u ovom dokumentu navedene su u tablici 1.

Kratica	**Definicija (HR)**
CA	certifikacijsko tijelo
DTBS	podaci koji se potpisuju
LTV	dugoročna valjanost
OID	identifikator objekta
SL	Službeni list Europske unije
PIN	osobni identifikacijski broj
OP	Ured za publikacije Europske unije
QC	kvalificirani certifikat
QESig	kvalificirani elektronički potpis
QESeal	kvalificirani elektronički pečat
QSCD	uređaj za izradu kvalificiranog potpisa/pečata
SAA	aplikacija za dopunjavanje potpisa
SCA	aplikacija za izradu potpisa
SSCD	uređaj za sigurnu izradu potpisa
SVA	aplikacija za provjeru valjanosti potpisa
TSP	pružatelj usluga povjerenja
QTSP	kvalificirani pružatelj usluga povjerenja
WIPIWIS	ono što je prikazano jest i potpisano

Tablica 1.: Definicije i kratice

2. Izjave o praksama u vezi s aplikacijama za potpisivanje

2.1. Povezani zahtjevi politike

Izdanja SL-a regulirana su člancima 1. i 2. Uredbe Vijeća o elektroničkom izdanju Službenog lista Europske unije, kojima je propisano, među ostalim, da elektroničko izdanje Službenog lista NOSI kvalificirani elektronički potpis definiran Uredbom (EU) br. 910/2014 Europskog parlamenta i Vijeća ili kvalificirani elektronički pečat definiran Uredbom (EU) br. 910/2014.

Elektroničko potpisivanje i pečaćenje izdanja SL-a pripada primjeni potpisivanja kao važne formalnosti navedene u članku III.2.1. PROVEDBENIH PRAVILA Europske komisije ZA ODLUKU 2002/47/EZ, EZUČ, EURATOM O UPRAVLJANJU DOKUMENTIMA I ZA ODLUKU 2004/563/EZ, EURATOM O ELEKTRONIČKIM I DIGITALNIM DOKUMENTIMA od 30. studenoga 2009.[2], koja isto tako nalažu da elektronički potpisi koji se primjenjuju na SL zahtijevaju kvalificirani elektronički potpis kako je utvrđeno u [eIDAS-u].

Prema članku III.2.3. PROVEDBENIH PRAVILA ZA ODLUKU 2002/47/EZ I ZA ODLUKU 2004/563/EZ[2] provjera ovlaštenog tijela za potpisivanje odgovornost je SCA-a za SL kada se osposobljava službenik OP-a za elektroničko potpisivanje izdanja SL-a ili kada se osposobljava OP kao pravna osoba za elektroničko pečaćenje izdanja SL-a.

Iako izdanja SL-a u elektroničkom obliku ne mogu imati pravni učinak bez potpisivanja ili pečaćenja, politika potpisivanja SL-a isto tako propisuje da SCA za SL JAMČI da samo ovlašteni potpisnici SL-a mogu odbiti izdanja SL-a kako bi se učinkovito spriječili napadi na postupak objave SL-a.

Budući da ovlašteni potpisnici SL-a djeluju u ime OP-a, odgovornost je glavnog urednika OP-a jamčiti (delegiranjem) pravilno odobrenje odgovarajućih QC-ova za potpisivanje SL-a. U tu svrhu odobrenja QC-a za potpisivanje SL-a:

- *MORAJU* biti pravilno konfigurirana u upravljanju korisnicima u SCA-u za SL,
- *TREBAJU* biti ograničena na zajedničke (profesionalne) certifikate kojima se jamči povezanost subjekta s OP-om[3],
- *MORAJU BITI* transparentna zahvaljujući objavljivanju odobrenog QC-a na internetskim stranicama EUR-Lex u skladu s člankom 2. Uredbe Vijeća o elektroničkom izdanju Službenog lista Europske unije.

2.2. Povezani pravni zahtjevi

Primjena elektroničkog potpisivanja i elektroničkog pečaćenja obuhvaćenog politikom potpisivanja SL-a UREĐUJE se sljedećim zakonskim odredbama:

- Uredbom Vijeća (EU) br. 216/2013 od 7. ožujka 2013. o elektroničkom izdanju Službenog lista Europske unije,
- Uredbom (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ[4],

[2] Vidjeti SEC(2009) 1643.

[3] Zajednički certifikati jamče povezanost subjekta s određenom organizacijom. Sigurnost je povećana jer QTSP izdavatelj zahtijeva dokaz o pravu korištenja određenog vlasnika certifikata.

[4] Vidjeti SL L 257, 28.8.2014., str. 73.

- 2009/767/EZ: Odlukom Komisije od 16. listopada 2009. o utvrđivanju mjera kojima se olakšava uporaba postupaka elektroničkim putem preko „jedinstvenih kontaktnih točaka" u skladu s Direktivom 2006/123/EZ Europskog parlamenta i Vijeća o uslugama na unutarnjem tržištu[5],
- Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)[6],
- Direktivom 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama)[7],
- Direktivom 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o izmjeni Direktive 2002/22/EZ o univerzalnim uslugama i pravima korisnika s obzirom na elektroničke komunikacijske mreže i usluge (Direktiva o univerzalnim uslugama), Direktive 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u sektoru elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) i Uredba (EZ) br. 2006/2004 o suradnji između nacionalnih tijela odgovornih za provedbu zakona o zaštiti potrošača[8],
- 2010/425/EU: Odlukom Komisije od 28. srpnja 2010. o izmjeni Odluke 2009/767/EZ o izradi, održavanju i objavi pouzdanih popisa pružatelja usluga certificiranja koje nadziru/akreditiraju države članice[9],
- 2009/496/EZ, EURATOM: Odlukom Europskog parlamenta, Vijeća, Komisije, Suda, Revizorskog suda, Gospodarskog i socijalnog odbora te Odbora regija od 26. lipnja 2009. o organizaciji i djelovanju Ureda za publikacije Europske unije[10],
- 2011/130/EU: Odlukom Komisije od 25. veljače 2011. o uspostavljanju minimalnih zahtjeva za prekograničnu obradu dokumenata koje elektronički potpisuju nadležna tijela prema Direktivi 2006/123/EZ Europskog parlamenta i Vijeća o uslugama na unutarnjem tržištu[3].

2.3. Tehničko-sigurnosne napomene

Kriptografski alati koji ispunjavaju uvjete za provedbu potpisivanja i pečaćenja SL-a MORAJU ispunjavati zahtjeve kvalificiranih elektroničkih potpisa prema definiciji u [eIDAS-u], u [ETSI 2016.] te u relevantnim suvremenim praksama.

2.4. Pravne napomene

Elektronički potpisi i pečati u izdanjima SL-a izrađuju se u ime OP-a na temelju Uredbe vijeća o elektroničkom izdanju Službenog lista Europske unije.

[5] Vidjeti SL L 274, 20.10.2009., str. 36.

[6] Vidjeti SL L 119, 4.5.2016., str. 1.

[7] Vidjeti SL L 201, 31.7.2002., str. 37.

[8] Vidjeti SL L 337, 18.12.2009., str. 11.

[9] Vidjeti SL L 199, 31.7.2010., str. 30.

[10] Vidjeti SL L 168, 30.6.2009., str. 41.

3. Parametri za utvrđivanje opsega djelovanja (BSP)

3.1. BSP-i uglavnom povezani s predmetnom aplikacijom/poslovnim procesom

3.1.1. BSP (a): postupak (slijed i vremenski raspored) potpisivanja

3.1.1.1. Opis općeg tijeka rada

OP objavljuje SL od ponedjeljka do petka, a moguća je i objava tijekom vikenda. Ta publikacija SL-a može biti izdanje SL-a ili izdanje akta SL-a. Izdanje SL-a višejezična je publikacija koja se sastoji od jednog ili više dokumenata. Svaka jezična verzija izdanja sadržava cjelokupan tekst svakog dokumenta u jednoj datoteci. Izdanje akta SL-a višejezična je publikacija samo jednog dokumenta koji se objavljuje samostalno. Svaka jezična verzija izdanja akta SL-a sadržava cjelokupan tekst svakog dokumenta u jednoj datoteci.

Pojedinačna se izdanja SL-a i akta SL-a kategoriziraju prema seriji kojoj pripadaju i kategorija je određujući dio SL-a. Značajne su dvije serije sadašnjeg opsega primjene, tj. L (zakonodavstvo) i C (informacije i napomene). Serije mogu imati i podserije i klasifikacijske sheme (vidjeti http://publications.europa.eu/code/hr/hr-10000.htm za detaljnije objašnjenje opsega primjene, strukture dokumenta i dodatne informacije o kontekstu).

Osim L i C serija SL-a, postoje i posebna izdanja objavljena na jeziku države pristupnice/nove države članice koja sadržavaju sekundarno zakonodavstvo EU-a. Ta su posebna izdanja isto tako dio područja primjene.

Čim izdanje SL-a ili akta SL-a bude potpuno (tj. kada sve jezične verzije izdanja SL-a ili akta SL-a budu dostupne u formatu PDF/A) i spremno za objavljivanje, slijedi postupak elektroničkog pečaćenja (vidjeti odjeljak 3.1.1.2.) odnosno postupak elektroničkog potpisivanja (vidjeti odjeljak 3.1.1.3.). U slučaju elektroničkog pečaćenja automatski se izrađuje kvalificirani elektronički pečat s pomoću kvalificiranog certifikata za elektronički pečat koji se izdaje OP-u kao tijelu Europske komisije. U slučaju elektroničkog potpisivanja kvalificirani elektronički potpis izrađuje ovlaštena osoba s pomoću kvalificiranog certifikata za elektronički potpis.

Elektroničko pečaćenje zadani je postupak koji odabire SCA, tj. potpuna izdanja SL-a ili akta SL-a prolaze kroz automatski postupak pečaćenja osim ako taj postupak nije dostupan. U potonjem slučaju primjenjuje se postupak potpisivanja.

Budući da se za potpisivanje svakog izdanja upotrebljava odvojeni XAdES potpis ili pečat s manifestom (vidjeti [Bartel 2008.], [ETSI 2022-XAdES] i 2011/130/EU: Odluku Komisije od 25. veljače 2011. o uspostavljanju minimalnih zahtjeva za prekograničnu obradu dokumenata koje elektronički potpisuju nadležna tijela prema Direktivi 2006/123/EZ Europskog parlamenta i Vijeća o uslugama na unutarnjem tržištu[11]), kada se provjerava potpis ili pečat SL-a ili akta SL-a, potrebno je provesti i provjeru valjanosti manifesta uz potpisnu osnovu XML-a (vidjeti [Bartel 2008.]) tijekom [ETSI 2022-XAdES] provjere valjanosti u svrhu provjere potpisa ili pečata SL-a ili akta SL-a.

U sljedećim pododjeljcima opisuju se postupci pečaćenja i potpisivanja visoke razine koji se primjenjuju u SCA-u, SAA-u i SVA-u za SL (vidjeti [ETSI 2016.]).

3.1.1.2. Izrada pečata SL-a i akta SL-a

1. Za pečaćenje se otkriva potpuno izdanje SL-a ili akta SL-a.
2. SCA obavlja početne provjere dostavljenih datoteka:

[11] SL L 53, 26.2.2011., str. 66.

a. provjerava postoje li razlike u veličini među različitim jezičnim verzijama izdanja SL-a ili akta SL-a i da su one unutar ograničenja veličine koja se mogu uređivati;

b. provjerava jesu li sve dostavljene jezične verzije bile predviđene za objavu.

3. U slučaju neuspješne provjere prekida se postupak pečaćenja. Za nastavak postupka pečaćenja potrebna je ručna intervencija ovlaštenog osoblja OP-a.

4. Nakon uspješne provjere SCA-a izrađuje se manifest u kojem se navodi svaka jezična verzija potpunog izdanja. Nadalje, svaka jezična verzija odgovara jednom od jezika EU-a i predstavljena je kao PDF/A dokument s kojim se postupa kao s nizom binarnih okteta za vrijeme izračuna sažetaka podataka.

5. SCA provjerava njezinu vjerodostojnost na središnjem portalu za elektroničko potpisivanje Europske komisije i prenosi izrađeni manifest radi automatiziranog pečaćenja.

6. Podneseni manifest pečati se putem portala za elektroničko potpisivanje s pomoću kvalificiranog certifikata za pečaćenje koji izdaje akreditirani europski QTSP (vidjeti [eIDAS]). Privatni ključ koji je povezan s tim certifikatom za pečaćenje pohranjen je na QSCD-u, koji je povezan s portalom za elektroničko potpisivanje.

7. XAdES pečat (vidjeti [ETSI 2022-XAdES]) koji se na taj način izradi zatim se vraća SCA-u, koji, među ostalim, provjerava valjanost upotrijebljenih algoritama i osigurava da je certifikat za pečaćenje dotičnog pečata odobren i u vlasništvu iste pravne osobe za koju je dokazano da je ovlašteni potpisnik.

8. Nakon uspješne provjere elektronički pečat dopunjuje se vremenskim žigom potpisa koji pruža akreditirani QTSP (vidjeti [eIDAS]).

9. Elektronički pečat dopunjen u prethodnom koraku u postupku prenosi se za objavu na internetskim stranicama EUR-Lex. Identična kopija pečata istodobno ostaje pohranjena u SCA-u.

10. Kad istekne obavezno 24-satno razdoblje čekanja za pečat koji se dobije u prethodnom koraku u postupku, pečat se dopunjuje u samoodrživ oblik kako bi potpis bio valjan dulje vrijeme, uz upotrebu pouzdane usluge izdavanja vremenskog žiga akreditiranog europskog QTSP-a (vidjeti [eIDAS]).

11. Pečat dopunjen u prethodnom koraku u postupku prenosi se za objavljivanje na internetskim stranicama EUR-Lex, zamjenjujući pritom pečat iz 9. koraka koji nije još dobio svoj samoodrživi oblik.

12. Osim objavljivanja na internetskim stranicama EUR-Lex, identične kopije dokumenata koji čine izdanje SL-a ili akta SL-a, zajedno s pripadajućim pečatom u samoodrživom obliku, prenose se u digitalni sustav za dugoročno čuvanje kojim upravlja OP i u kojem se dugoročno čuvaju službeni dokumenti institucija EU-a. Aspekti primjene koji se odnose na dugoročno čuvanje NISU obuhvaćeni ovom politikom potpisivanja.

3.1.1.3. Izrada potpisa SL-a i akta SL-a

1. Za potpisivanje se otkriva potpuno izdanje SL-a ili akta SL-a.

2. Izrađuje se manifest u kojem se navodi svaka jezična verzija potpunog izdanja. Nadalje, svaka jezična verzija odgovara jednom od jezika EU-a i predstavljena je kao PDF/A dokument s kojim se postupa kao nizom binarnih okteta za vrijeme izračuna sažetaka podataka.

Napominjemo da cijelim izdanjem ekskluzivno upravlja i zaključava ga SCA tijekom izrade manifesta kako bi se jamčio dosljedan izračun sažetka, koji je ključan za ovaj postupak.

3. Nakon SCA-ove uspješne provjere vjerodostojnosti, ovlašteni potpisnik može odabrati cjelokupno izdanje za potpisivanje, pod uvjetom da je odgovarajući manifest izrađen tijekom prethodnog koraka.
4. Nakon uspješnog odabira izdanja za potpisivanje, ovlašteni potpisnik počinje s postupkom potpisivanja tog izdanja.
    a. Kako bi se u potpunosti poštovalo načelo WIPIWIS-a, ovlašteni potpisnik mora ispitati najmanje tri različite jezične verzije, koristeći odgovarajući PDF/A preglednik prije samog potpisivanja izdanja. Ako izdanje SL-a ili akta SL-a ima manje od tri jezične verzije, tada ovlašteni potpisnik mora ispitati sve dostupne jezične verzije.

        Napominjemo da SCA omogućava potpisnicima pregled bilo koje jezične verzije koja se potpisuje. Potpisnik MOŽE pregledati cjelokupni sadržaj koji se potpisuje, ako to želi.

    b. Ovlašteni potpisnik može promišljeno odabrati hoće li odbiti izdanje, čime se prekida postupak potpisivanja ili će nastaviti s potpisivanjem pritiskom na tipku Potpiši.
    c. Nakon pritiska na tipku Potpiši:
        i. SCA izrađuje zahtjev za potpisivanje upućen središnjem portalu za elektroničko potpisivanje Europske komisije te prenosi manifest radi potpisivanja i preusmjerava ovlaštenog potpisnika na portal;
        ii. ovlašteni potpisnik provjerava vjerodostojnost putem portala za elektroničko potpisivanje i dodjeljuje mu se manifest radi potpisivanja prema načelima WIPIWIS-a;
        iii. portal za elektroničko potpisivanje povezuje se s posredničkim softverom instaliranim na radnoj stanici ovlaštenog potpisnika i dohvaća potpisnikov kvalificirani certifikat za potpisivanje koji izdaje akreditirani europski QTSP (vidjeti [eIDAS]). Taj se certifikat dodjeljuje ovlaštenom potpisniku koji tada mora unijeti odgovarajući PIN kojim je zaštićen QSCD kako bi ovlastio QSCD za izradu potpisa s pomoću privatnog ključa koji odgovara odabranom certifikatu za potpisivanje te time završava postupak potpisivanja.
    d. Posrednički softver šalje izrađenu vrijednost potpisa portalu za elektroničko potpisivanje, koji zatim izrađuje pripadajući XAdES potpis (vidjeti [ETSI 2022-XAdES]).
5. XAdES potpis zatim se vraća SCA-u, koji putem portala za elektroničko potpisivanje među ostalim provjerava valjanost upotrijebljenih algoritama i osigurava da je certifikat za potpisivanje predmetnog potpisa odobren i u vlasništvu iste osobe za koju je dokazano da je ovlašteni potpisnik.
6. Nakon uspješne provjere potpis se putem portala za elektroničko potpisivanje dopunjuje vremenskim žigom potpisa koji dodjeljuje akreditirani QTSP (vidjeti [eIDAS]).
7. Potpis dopunjen tijekom prethodnog koraka u postupku prenosi se za objavu na internetskim stranicama EUR-Lex. Identična kopija potpisa istodobno ostaje pohranjena u SCA-u.

8. Kad istekne obvezno 24-satno razdoblje čekanja za potpis koji se dobije u prethodnom koraku u postupku, potpis se dopunjuje u samoodrživ oblik kako bi bio valjan dulje vrijeme, uz upotrebu pouzdane usluge izdavanja vremenskog žiga akreditiranog europskog QTSP-a (vidjeti [eIDAS]).
9. Potpis dopunjen tijekom prethodnog koraka u postupku prenosi se za objavljivanje na internetskim stranicama EUR-Lex, zamjenjujući pritom potpis iz 7. koraka koji još nije dobio svoj samoodrživi oblik.
10. Osim objavljivanja na internetskim stranicama EUR-Lex, identične kopije dokumenata koji čine izdanje SL-a ili akta SL-a, zajedno s pripadajućim potpisom u samoodrživom obliku, prenose se u digitalni sustav za dugoročno čuvanje kojim upravlja OP i u kojem se dugoročno čuvaju službeni dokumenti institucija EU-a. Aspekti primjene koji se odnose na dugoročno čuvanje NISU obuhvaćeni ovom politikom potpisivanja.

3.1.1.4. Izvanredna situacija

Ako nije moguće izraditi pečat ili potpis SL-a ili akta SL-a kao što je opisano u odjeljku 3.1.1.2. ili 3.1.1.3. zbog nepredviđene i iznimne nedostupnosti SCA-a za SL, Ured za publikacije stavit će QESeal ili QESig na svaki PDF/A dokument koji odgovara svakoj jezičnoj verziji izdanja SL-a ili akta SL-a. Svi PDF/A dokumenti s pečatom ili potpisom prenose se za objavljivanje na internetskim stranicama EUR-Lex.

3.1.2. BSP (b): podaci koji se potpisuju

- Potpisi i pečati SL-a ili akta SL-a ovise o manifestu XML-a (vidjeti [Bartel 2008.] i [ETSI 2022-XAdES]) koji kombinira sve jezične verzije dostupne u formatu PDF/A koji se odnosi na jedno izdanje SL-a ili akta SL-a u jednom potpisu koji mora ispunjavati sljedeće zahtjeve: svaka jezična verzija koja je logički povezana s nekim izdanjem SL-a ili akta SL-a *MORA* imati vlastitu vrijednost sažetka,
- sve jezične verzije koje su logički povezane s nekim izdanjem SL-a ili akta SL-a MORAJU se dati na uvid potpisniku tijekom izrade potpisa, tako da potpisnik može pregledati sadržaj potpisa i provjeriti ga prema vlastitom nahođenju, kao što je opisano u odjeljku 3.1.1.3., radi poštovanja načela WIPIWIS-a,
- pravilna se vizualizacija *MORA* jamčiti upotrebom softvera za čitanje koji podržava format PDF/A,
- samo jezične varijante koje se odnose na određeno izdanje koje se potpisuje DAJU se na uvid potpisniku tijekom procesa potpisivanja,
- tehnička svojstva svih jezičnih verzija koje su logički povezane s nekim izdanjem SL-a ili akta SL-a MORAJU se provjeriti tijekom izrade pečata i potpisa kako bi se osigurala dosljednost.

U slučaju izvanredne situacije, kako je opisano u odjeljku 3.1.1.4., primjenjuju se sljedeći zahtjevi:

- svaka jezična verzija izdanja SL-a ili akta SL-a *MORA* imati QESeal ili QESig,
- sve jezične verzije koje su logički povezane s nekim izdanjem SL-a ili akta SL-a MORA pregledati potpisnik tijekom izrade potpisa tako da može provjeriti sadržaj potpisa prema vlastitom nahođenju radi poštovanja načela WIPIWIS-a,
- pravilna se vizualizacija *MORA* jamčiti upotrebom softvera za čitanje koji podržava format PDF/A.

3.1.3. BSP (c): veza između potpisanih podataka i potpisa i pečata

Potpis ili pečat SL-a ili akta SL-a vrijedi za sve jezične verzije jednog izdanja SL-a ili akta SL-a, od kojih svaka ima oblik PDF/A dokumenta.

Tijekom izrade potpisa ili pečata SL-a ili akta SL-a digitalni sadržaj dokumenta koji se potpisuje/pečati sažima se kao binarni niz okteta s pomoću najjačeg podržanog algoritma sažimanja koji je u skladu s odjeljkom 7.3. dokumenta [ETSI 2022-Crypto].

Pojedinačne vrijednosti sažetka dokumenta kombiniraju se zajedno s URI-jevima izvornih naziva datoteka u manifestu XML-a bez dodatnih preoblikovanja (vidjeti [Bartel 2008.]).

Manifest, uključujući potpisane atribute, potpisuje se ili pečati s pomoću XAdES-a (vidjeti [ETSI 2022-XAdES]) s obzirom na profil naveden u Odluci Komisije 2011/130/EU od 25. veljače 2013.

U slučaju izvanredne situacije, kako je opisano u odjeljku 3.1.1.4., svaki PDF/A dokument koji predstavlja svaku jezičnu verziju izdanja SL-a ili akta SL-a potpisuje se ili pečati s pomoću PAdES-a (vidjeti [ETSI 2016-PAdES] [eIDAS]).

3.1.4. BSP (d): ciljana zajednica

Ciljana zajednica je bilo koja strana koja se oslanja na autentičnost SL-a i treba je provjeriti, kao i sve strane odgovorne za provedbu SCA-a i SAA-a koji se upotrebljavaju za izradu e-potpisa ili e-pečata, kao i za njihovo dopunjavanje za izdanja SL-a ili akta SL-a.

3.1.5. BSP (e): raspodjela odgovornosti za provjeru valjanosti i dopunjavanje potpisa

3.1.5.1. Provjera potpisa i pečata SL-a ili akta SL-a

Svaka pouzdajuća strana, naročito građani EU-a, može preuzeti izdanje SL-a ili akta SL-a objavljeno na internetskim stranicama EUR-Lex i odgovarajući odvojeni XAdES potpis ili pečat (vidjeti [ETSI 2022-XAdES]) radi provjere.

Budući da se tijekom izrade potpisa i pečata upotrebljavaju interoperabilni europski standard za potpisivanje i usluge akreditiranog europskog QTSP-a (vidjeti [eIDAS]), provjera se može obaviti s pomoću bilo kojeg alata za provjeru treće strane koji je u skladu s primijenjenim standardima, uz uvjet da se provjera valjanosti manifesta može obaviti na temelju politike potpisivanja SL-a.

U slučaju izvanredne situacije, kako je opisano u odjeljku 3.1.1.4., svaki PDF/A dokument koji predstavlja svaku jezičnu verziju izdanja SL-a ili akta SL-a potpisuje se ili pečati s pomoću PAdES-a (vidjeti [ETSI 2016-PAdES]). Njihova se provjera može obaviti s pomoću bilo kojeg alata za provjeru treće strane koji je u skladu s primijenjenim standardom.

3.1.5.1.1. Provjera na serveru

Kako bi se olakšala provjera potpisa i pečata, OP MOŽE ponuditi besplatan SVA za SL na serveru koji funkcionira u skladu s postupkom provjere navedenim u nastavku:

1. vršitelj provjere učitava PDF/A datoteku koja se provjerava i povezanu datoteku s potpisom ili pečatom primjenom funkcije učitavanja datoteka koju omogućava SVA;
2. SVA izračunava sažetak učitane PDF/A datoteke i provjerava je li izračunani sažetak sadržan u manifestu učitanog potpisa;
3. nakon uspješne provjere sažetka provodi se standardna XAdES provjera učitanog kandidatskog potpisa ili pečata, pod uvjetom da certifikat za potpisivanje ili pečaćenje identificira ovlaštenog potpisnika SL-a za razdoblje određeno vremenskim žigom potpisa. SVA-om se provjerava i je li potpisnik bio ovlašten u trenutku izrade potpisa prema vremenskom žigu potpisa;
4. provjera se smatra uspješnom ako su svi prethodni koraci uspješno provedeni. U protivnom se provjera smatra neuspješnom. U svakom slučaju, sveobuhvatni izvještaj o postupku provjere mora se dati na uvid vršitelju provjere.

3.1.5.1.2. Provjera klijenta

Kako bi se olakšala provjera potpisa i pečata, OP MOŽE ponuditi besplatan SVA za SL kod klijenta koji funkcionira u skladu s postupkom provjere navedenim u nastavku:

1. vršitelj provjere pokreće preuzeti SVA, njegov potpis koda automatski se provjerava u izvršnom okruženju i provedbu odobrava vršitelj provjere nakon uspješne provjere potpisa koda;
2. vršitelj provjere odabire PDF/A datoteku u određenoj jezičnoj verziji koja će se provjeriti uz povezanu datoteku kandidatskog potpisa ili pečata na lokalnom računalnom datotečnom sustavu s pomoću dijaloga za odabir datoteka koji omogućava SVA;
3. SVA izračunava sažetak odabranog dokumenta i provjerava je li izračunani sažetak sadržan u manifestu odabranog kandidatskog potpisa ili pečata;
4. nakon uspješne provjere sažetka provodi se uobičajena XAdES provjera odabranog kandidatskog potpisa ili pečata;
5. provjera se smatra uspješnom ako su svi prethodni koraci uspješno završeni i ako certifikat za potpisivanje ili pečaćenje identificira ovlaštenog potpisnika SL-a za razdoblje određeno vremenskim žigom potpisa.

   Napominjemo da odobrene informacije o potpisniku POZNATE su SVA-i na temelju (zadane) konfiguracije. Međutim, sažetak certifikata za potpisivanje ili pečaćenje dodatno se naznačuje u rezultatima SVA-a, tako da ih vršitelj provjere može ručno usporediti s objavljenim pravnim informacijama o potpisniku tijekom razdoblja izrade potpisa ili pečata, koji su isto tako navedeni u rezultatima SVA-a.

3.2. BSP-i na koje uglavnom utječu zakonske/regulatorne odredbe u vezi s predmetnom aplikacijom/poslovnim procesom

3.2.1. BSP (f): pravni oblik potpisa

Elektronički potpisi i pečati u SL-u ili aktu SL-a JESU QESig i QESeal u smislu [eIDAS-a].

Prethodno navedeni uvjet propisan je ponajprije Uredbom Vijeća o elektroničkom izdanju Službenog lista Europske unije (vidjeti odjeljak 2.2.).

QC se mora dobiti za svakog potpisnika, što je preduvjet za korištenje sustavom za potpisivanje.

Kvaliteta posebnih elemenata traženog QESig-a i QESeal-a MORA zadovoljavati sljedeće zahtjeve u pogledu kvalitete:

- uređaj za potpisivanje i pečaćenje: QSCD-i usklađeni s Prilogom II. [eIDAS-u],
- izdavanje certifikata: QC usklađen s Prilogom I. [eIDAS-u],
- nezavisno jamstvo za izdavanje certifikata: QC koji izdaje nadzirani ili akreditirani pružatelj certifikacijskih usluga QTSP-a akreditiran u bilo kojoj zemlji u kojoj se primjenjuje [eIDAS],
- kriptografski potpis: upotrebljavaju se samo potpisi navedeni u odjeljku 7.3. dokumenta [ETSI 2022-Crypto],
- rješenja LTV-a: oblici potpisa XAdES (vidjeti [ETSI 2022-XAdES]) i pečata za SL ili akt SL-a DOPUNJENI su do oblika -LTA uključujući obnovu arhivskih vremenskih žigova ili drugih oznaka (vanjski sigurni arhivski mehanizmi MOGU se smatrati alternativom obnovi arhivskih vremenskih žigova, pod uvjetom da su jednake ili bolje kvalitete),

- aplikacija za izradu potpisa: kvaliteta SCA-a za SL ISPUNJAVA zahtjeve u pogledu kvalitete koji su propisani politikama EZ-a i usklađeni s odredbama Uredbe Vijeća o elektroničkom izdanju Službenog lista Europske unije.

3.2.2. BSP (g): obvezakoju preuzima potpisnik

Elektronički potpisi i pečati u izdanjima SL-a ili akta SL-a IZRAĐUJU se u ime OP-a u skladu s Uredbom vijeća o elektroničkom izdanju Službenog lista Europske unije.

Predanost ovlaštenog potpisnika SL-a označava da potpisani podaci predstavljaju vjerodostojno izdanje SL-a ili akta SL-a, čija se provjera valjanosti izvršila s obzirom na pravila o opsegu poslovne primjene (vidi odjeljak 3.1.1.) i koje je objavio OP u skladu s Uredbom Vijeća o elektroničkim publikacijama Službenog lista Europske unije, kako bi se njime moglo služiti kao istinskim izvorom prava EU-a.

U potpisu SL-a NE SMIJE biti uključena izričita oznaka o vrsti obveze (vidjeti odjeljak 5.2.3. u [ETSI 2022-XAdES]).

3.2.3. BSP (h): razina jamstva za dokaze o vremenskom rasporedu

Vremenski žig potpisa DODAJE se potpisima ili pečatima SL-a ili akta SL-a koji su izrađeni kako je opisano u odjeljku 3.1.1.2. ili 3.1.1.3. istog dana (prema lokalnom vremenu u Luksemburgu) kao i potpis ili pečat u izdanju SL-a ili akta SL-a kako bi se potvrdilo da potpis ili pečat nije izrađen nakon datuma objave. Time se osigurava da je skup ovlaštenih potpisnika koji je primjenjiv na datum objave primjenjiv i za potpis ili pečat.

SCA za SL OSIGURAVA da svi potpisi XAdES-B-T koji se izrađuju ispunjavaju taj zahtjev.

Vremenski žig koji se upotrebljava radi izrade vremenskih žigova potpisa u potpisima XAdES-B-T kvalificirani JE vremenski žig.

Potpisi PAdES izrađeni u slučaju izvanredne situacije, kako je opisano u odjeljku 3.1.1.4. MOGU se izrađivati bez vremenskog žiga potpisa.

Ako su potpisi PAdES izrađeni u slučaju izvanredne situacije kako je opisano u odjeljku 3.1.1.4. izrađeni s vremenskim žigom potpisa, vremenski žig potpisa TREBA biti kvalificirani vremenski žig i primjenjuje se istog dana (prema lokalnom vremenu u Luxembourgu) kao i potpis ili pečat u izdanju SL-a ili akta SL-a kako bi se potvrdilo da potpis ili pečat nije izrađen nakon datuma objave.

NAPOMENA: To znači da u slučaju izvanredne situacije, ako je vremenski žig potpisa uključen u potpis, on može biti nekvalificirani vremenski žig.

Svi ostali vremenski žigovi, uključujući arhivske vremenske žigove i vremenske žigove sadržaja, ako postoje, TREBAJU biti kvalificirani vremenski žigovi.

3.2.4. BSP (i): formalnosti pri potpisivanju

Odgovornost je SCA-a za SL osigurati sučelje za potpisnike na način kojim će jamčiti, koliko je to moguće, odgovarajuće pravno okruženje za potpis ili pečat. Sučelje mora:

- sadržavati odgovarajuće upute i informacije o postupku potpisivanja ili pečaćenja u aplikaciji,
- osigurati dosljednost između upotrebe odgovarajuće izrade potpisa i pečata i podataka za provjeru, uređaja za izradu potpisa i pečata, podataka koji se potpisuju i očekivanog opsega i svrhe potpisivanja i pečaćenja (ili samog čina potpisivanja ili pečaćenja),
- omogućiti i pokazati jasan izraz volje za potpisivanjem i korisnikovu namjeru da bude obvezan potpisom ili pečatom,
- omogućiti i prikazati informirani pristanak.

SVA za SL OSIGURAVA pouzdajućim stranama (i potpisniku) odgovarajuće postupke provjere i arhiviranja elektroničkih potpisa ili pečata i podataka za provjeru.

3.2.5. BSP (j): dugotrajnost i otpornost na izmjene

Potpisana izdanja SL-a ili akta SL-a i njihovi potpisi MORAJU se čuvati tijekom neodređenog vremenskog razdoblja. Očuvanje valjanosti potpisa SL-a ili akta SL-a MORA biti osigurano u navedenom vremenskom razdoblju (vidjeti članak 2. Uredbe Vijeća o elektroničkom izdanju Službenog lista Europske unije).

3.2.6. BSP (k): arhiviranje

Nije primjenjivo.

3.3. BSP-i uglavnom povezani s dionicima u izradi/dopunjavanju/provjeri valjanosti potpisa

3.3.1. BSP (l): identitet (i uloge/atributi) potpisnika

3.3.1.1. Prijedlog pravila za potpisnike i identifikaciju

Potpise SL-a ili akta SL-a PRIMJENJUJU ovlašteni potpisnici, koji postaju službenici OP-a posjedovanjem potrebne stručnosti za provjeru valjanosti izdanja SL-a ili akta SL-a u skladu s pravilima koja se odnose na opseg poslovne primjene (vidi odjeljak 3.1.1.3.). U slučaju pečata SL-a ili akta SL-a ovlašteni potpisnik JEST sâm OP kao tijelo Europske komisije.

Ovlašteni potpisnici SVJESNI su svoje odgovornosti i DJELUJU vjerno ovjeravajući pravne tekstove koji predstavljaju pravo EU-a.

Veza između fizičkih osoba potpisnika i njihovih podataka za provjeru potpisa PROVJERAVA se u QC-u s obzirom na [eIDAS], čime se potvrđuje njihov identitet i poveznica s OP-om.

Odobrenje potpisnika SL-a obavlja glavni urednik OP-a (ili njegov izaslanik).

3.3.1.2. Karakteristike i uloge potpisnika

Daljnji atributi uloge, funkcije ili kvalifikacija NE ZAHTIJEVAJU certificiranje u QC-u potpisnika, osim poveznice potpisnika s OP-om.

ODGOVORNOST je SCA-a za SL osigurati odgovarajuću kontrolu pristupa i ovlaštenje potpisnika prije davanja pristupa potpisnicima mjestu potpisivanja u AOJ-u.

Kontrola pristupa i ovlaštenje potpisnika OBAVLJA se na temelju snažnog mehanizma ovjere koji se provodi u SCA-u i uz dozvolu prijavljenu uporabom javnog ključa certifikata za ovlaštene potpisnike u bazi podataka SCA-a za upravljanje korisnicima.

Pouzdajuće strane *MOGU* upotrijebiti objavljene certifikate potpisnika SL-a za provjeru svojih zakonskih ovlasti.

3.3.1.3. Povezani dokaz o ovlaštenju

Nema daljnjih odredaba osim onih navedenih u odjeljku 3.3.1.2.

3.3.2. BSP (m): razina jamstva potrebna za provjeru vjerodostojnosti potpisnika

Razina jamstva potrebna za provjeru vjerodostojnosti potpisnika osigurana je njegovim kvalificiranim certifikatom i sredstvom za izradu potpisa, odnosno uređajem za izradu kvalificiranog potpisa/pečata kako je definirano u [eIDAS].

3.4. Ostali BSP-i

3.4.1. BSP (o): druge informacije povezane s potpisom ili pečatom

3.4.1.1. Ovjereni potpisnici SL-a i tijela za izdavanje vremenskih žigova

Provjeravanje ovlaštenja potpisnika je ključan element povjerenja AOJ-a.

Ovlaštenje se DAJE izričito objavljivanjem elektroničkih certifikata svih ovlaštenih potpisnika putem pouzdanog medija izvan SCA-a/SVA-a.

Objavljivanje ovlaštenih potpisnika SL-a ZNAČI da je nadzorni status certifikata potpisnika zajamčen za tekuće razdoblje potpisivanja SL-a ili akta SL-a.

Ovlašteni potpisnici SL-a i tijela za izdavanje vremenskih žigova NE OBJAVLJUJU se u SL-u jer bi se time mogli pojaviti problemi s kružnim zaključivanjem, naročito u pogledu dugoročne provjere valjanosti.

Kad se ovlašteni potpisnici SL-a promijene s vremenom, prethodna skupina potpisnika OBJAVLJUJE se kao povijesna informacija od povjerenja. Ovo je potrebno za provjeru izdanja SL-a ili akta SL-a koja potpisuju ovi potpisnici.

Publikacije ovlaštenih potpisnika SADRŽAVAJU razdoblje tijekom kojeg su navedeni potpisnici bili ili jesu ovlašteni, a ta napomena mora biti u skladu s vremenskim ograničenjima ove verzije politike.

3.4.1.2. Pravila o atributima, opsegu i svrsi elektroničkog potpisivanja i pečaćenja

U postupcima izrade potpisa i pečata na odgovarajući se način PRIMJENJUJU atributi potpisa, posebice potpisani atributi koji su informacije koje podržavaju elektronički potpis/pečat, a koji su obuhvaćeni potpisom/pečatom zajedno s DTBS-om u skladu sa sljedećim:

- UPOTREBLJAVA se identifikator potpisnog certifikata. To je identifikator ili referenca certifikata koji sadržava podatke o provjeri potpisa koji odgovaraju podacima o izradi potpisa ili pečata koje je potpisnik upotrijebio za izradu elektroničkog potpisa ili pečata,
- MOŽE se upotrijebiti pokazatelj politike potpisivanja (vidjeti odjeljak 1.2.2.),
- PRIMJENJUJE se navedeno vrijeme potpisivanja. Ono ukazuje na vrijeme kad potpisnik tvrdi da je izradio potpis ili pečat.

  Napominjemo da se vrijeme određuje prema trenutačnom vremenu sustava na radnoj stanici potpisnika. To se NE smatra pouzdanim vremenom.

  Vlasnik SCA-a za SL (kojeg delegira glavni direktor OP-a) OSIGURAVA da je vrijeme na radnim stanicama potpisnika ispravno namješteno.

  To se može postići upotrebom NTP-a s odgovarajućim izvorom mjerenja vremena (vidjeti [*Mills 2010*.]);

- NE UPOTREBLJAVA se nikakva oznaka o vrsti obveze,
- MOGU se upotrijebiti drugi potpisani atributi.

Upotreba atributa potpisa MORA biti u skladu s [ETSI 2010.] i Odlukom Komisije 2011/130/EU od 25. veljače 2013.

3.4.2. BSP (p): kriptografski potpisi

Vidjeti odjeljak 3.2.1.

4. Zahtjevi/izjave o provedbi tehničkih mehanizama i standarda

4.1. Pravila o pouzdanim vremenskim žigovima

Oblik potpisa XAdES-B-LTA (vidjeti [ETSI 2022-XAdES]) zahtijeva više vremenskih žigova koji se DOBIVAJU od kvalificiranog pružatelja usluga za izdavanje vremenskih žigova akreditiranog u državi članici EU-a ili EGP-a.

Vlasnik SCA-a za SL (kojeg delegira glavni direktor OP-a) OSIGURAVA da se SCA konfigurira za upotrebu prikladnih kriptografskih algoritama.

4.2. Pravila o dugoročnoj valjanosti

Očuvanje valjanosti potpisa SL-a ili akta SL-a tijekom očekivanog razdoblja čuvanja osigurava se primjenom oblika potpisa XAdES-B-LTA (vidjeti [ETSI 2022-XAdES]) i kasnijim dopunjavanjem potpisa dodatnim kvalificiranim arhivskim vremenskim žigom kako bi se prema potrebi produljila njegova valjanost ili odgovarajućim arhivskim rješenjem koje pruža jamstva očuvanja valjanosti potpisa.

4.3. Ostala poslovna i pravna pitanja

Budući da se SL objavljuje od ponedjeljka do petka, a moguće i vikendom, vlasnik SCA-a za SL (kojeg delegira glavni direktor OP-a) MORA osigurati da SCA bude neprekidno u funkciji.

U tu se svrhu TREBAJU uspostaviti odgovarajući sporazumi o razini usluga.

Iako potpise i pečate SL-a ili akta SL-a može provjeriti bilo koji SVA u skladu s normama i pravilima definiranima u politici potpisivanja SL-a, koja isto tako zahtijeva provjeru valjanosti manifesta, OP MOŽE izložiti javno raspoloživ SVA na internetskim stranicama EUR-Lex kako bi omogućio pouzdajućim stranama, naročito građanima EU-a, provjeru potpisa SL-a ili akta SL-a bez upotrebe alata treće strane.

OP MOŽE, prema potrebi, osigurati SVA kao javno raspoloživu samostalnu aplikaciju na radnoj površini računala korisnika, koja zahtijeva da se tijekom provjere vršitelj provjere pouzda u softver i u rezultate koji se njime dobiju.

5. Dodatak

[Bartel 2008.]	Bartel M., Boyer J., Fox B., LaMacchia B., Simon E. *XML Signature Syntax and Processing (Second Edition)* W3C Recommendation, 2008.
[Bradner 1997.]	Bradner S. *Key words for use in RFCs to indicate requirement levels* RFC 2119, Network Working Group, 1997.
[Mealling 2010.]	Mealling M. *A URN Namespace of Object Identifiers* RFC 3061, Network Working Group, 2001.
[Mills 2010.]	Mills D., Delaware U., Martin J., ISC Ed., Burbank J., Kasch W. *Network Time Protocol Version 4: Protocol and Algorithms Specification* RFC 5905, IETF, 2010.
[eIDAS]	*Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ* Službeni list L 257
[ETSI 2015.]	ETSI-ESI *Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents* TS 119 172-1, v1.1.1, ETSI, 2015.
[ETSI 2016.]	ETSI-ESI *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation* TS 119 101, v1.1.1, ETSI, 2016.
[ETSI 2016-PAdES]	ETSI-ESI *PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures* ETSI EN 319 142-1 V1.1.1 (2016-04)
[ETSI 2022-XAdES]	ETSI-ESI *XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures* ETSI EN 319 132-1 V1.2.1 (2022-02)
[ETSI 2022-Crypto]	ETSI-ESI Cryptographic Suites ETSI TS 119 312 V1.4.2 (2022-02)