ePotpis

Tehnička specifikacija za integraciju pružatelja e-Usluga

VERZIJA: 4.0.14

https://developer.certilia.com

1 UVOD 1

1.1 REFERENCE 2

2 PODACI PRUŽATELJA E-USLUGE 3

2.1 NAZIV PRUŽATELJA E-USLUGA (NPR. ORGANIZACIJA A) 3
2.2 NAZIV E-USLUGE (NPR. E-ZAHTJEV) 3
2.3 NAZIVI DOKUMENATA (NPR. ZAHTJEV ZA UPIS U…) 3
2.4 BAZNI URL KLIJENTA 3
2.5 URL NA KOJEM SE NALAZI POTPIS PDF-A SA KLIJENTSKE STRANE 3
2.6 URL NA KOJI SE PREUSMJERUJE NAKON USPJEŠNOG POTPISA 4
2.7 URL NA KOJI SE PREUSMJERUJE KAD DOĐE DO GREŠKE 4
2.8 (OPCIJA) BAZNI URL NA KOJEM USLUGA SKLADIŠTI POTPISANE DOKUMENTE ZA POTREBE DOHVATA KOD VERIFIKACIJE 4
2.9 ADRESE SERVERA E-USLUGE 4
2.10 OSOBA ZA ADMINISTRACIJU PUTEM CERTILIA DEVELOPER PORTALA 4

3 PREDUVJETI ZA INTEGRACIJU 5

3.1 MREŽNI PREDUVJETI 5
3.2 IDENTIFIKACIJSKI PODACI ZA KORIŠTENJE EPOTPIS RJEŠENJA 5
3.3 POTPISNI CERTIFIKATI 5
3.4 PROGRAMSKI PAKET ZA RAD S PAMETNOM KARTICOM - MIDDLEWARE 6
3.5 URL AKD SERVISA ZA PROVJERU STATUSA CERTIFIKATA I TSA 6
3.5.1 CertiliaCA 6
3.5.2 KIDCA 7
3.5.3 HRIDCA 8
3.5.4 TSA 9

4 OPIS EPOTPIS RJEŠENJA 10

4.1 KOMPONENTE AKD EPOTPIS RJEŠENJA 10
4.1.1 ePotpis 10
4.1.2 PAdES/XAdES web api 10
4.2 FUNKCIONALNOSTI EPOTPIS RJEŠENJA 10
4.3 DIJAGRAM TOKA KOMUNIKACIJE KOMPONENTI 11

5 INTEGRACIJSKE KOMPONENTE 14

5.1 DEFINICIJE 14
5.1.1 Potpis 14
5.1.2 Pečat 14
5.1.3 Token 14
5.1.4 Verifikacijski kod 15
5.1.5 Vizual 15
5.1.6 PersonNaturalData 15
5.1.7 PersonLegalData 15
5.2 EPOTPIS 17
5.2.1 Zaprimanje inicijalnih podataka za potpis 17
5.2.1.1 Primjer 1a – Zaprimanje inicijalnih podataka kod potpisivanja jednog dokumenta 17
5.2.1.1.1 Upit 17
5.2.1.1.2 Odgovor 18
5.2.1.1.3 Odgovor u slučaju GREŠKE 18
5.2.1.2 Primjer 1b – Zaprimanje inicijalnih podataka kod potpisivanja više dokumenta 18
5.2.1.2.1 Upit 19
5.2.1.2.2 Odgovor 19
5.2.1.2.3 Odgovor u slučaju greške 19
5.2.2 Zaprimanje hash-a dokumenta za potpis 21
5.2.2.1 Primjer 2 – Zaprimanje hash-a za jedan dokument 21
5.2.2.1.1 *Upit* 21
5.2.2.1.2 Odgovor 22
5.2.2.1.3 Odgovor u slučaju greške 22

5.2.3 Preusmjeravanje korisnika na potpisno rješenje 23
5.2.4 Vraćanje potpisanih podataka 24
5.2.4.1 Primjer 3 – Vraćanje potpisanih podataka 24
5.2.4.1.1 Upit 24
5.2.4.1.2 Odgovor 25
5.2.4.1.3 Odgovor u slučaju greške 25
5.2.4.2 Korisnik je odbio potpisivanje putem mobilne aplikacija 25
5.3 AdES (PAdES / XAdES) WEB API 26
5.3.1 Tehnički preduvjeti 26
5.3.1.1 Postavke sustava 26
5.3.1.2 Podaci za AKD TimeStamp servis 26
5.3.2 Osnovne funkcionalnosti 27
5.3.3 Ograničenja i preporuke za korištenje servisa 27
5.3.4 Napomene 28
5.3.4.1 Dodavanje prazne stranice (PAdES) 28
5.3.4.2 Vizual (PAdES) 28
5.3.4.2.1 Vrste vizuala 29
5.3.5 WEB API parametri 30
5.3.5.1 PAdES parametri 30
5.3.5.1.1 Metoda POST za izračun HASH vrijednosti 30
5.3.5.1.2 Metoda PATCH za ugradnju potpisa 33
5.3.5.2 XAdES parametri 36
5.3.5.2.1 Metoda POST za izračun HASH vrijednosti 36
5.3.5.2.2 Metoda PATCH za ugradnju potpisa 38
5.3.5.3 PAdES Web API primjeri 41
5.3.5.3.1 Računanje hash vrijednosti PDF dokumenta (PreSign) 41
5.3.5.3.2 Upit 41
5.3.5.3.3 Odgovor 42
5.3.5.3.4 Ugradnja potpisane vrijednosti u PDF dokument (PostSign) 42
5.3.5.3.5 Upit 43
5.3.5.3.6 Odgovor 44
5.3.5.4 XAdES Web API primjeri 45
5.3.5.4.1 Računanje hash vrijednosti XML dokumenta (PreSign) 45
5.3.5.4.2 Upit 45
5.3.5.4.3 Odgovor 46
5.3.5.4.4 Ugradnja potpisane vrijednosti u XML dokument (PostSign) 46
5.3.5.4.5 Upit 47
5.3.5.4.6 Odgovor 48
5.3.6 Provjera potpisa u Acrobat Readeru 49
5.3.7 Greške 52
5.3.7.1 PAdES 53
5.3.7.2 XAdES 55

6 PRILOZI 58

6.1 Prilog A – Lokacije vizualnog elementa unutar A4 stranice 58
6.2 Prilog B – Elementi standardnog vizuala 64
6.3 Prilog C – Elementi vizuala 'small' 65

Revizija dokumenta

Oznaka verzije	Datum revizije	Autor	Opis izmjene
1.0	18.9.2017	AKD	Prvo izdanje dokumenta
2.0	14.12.2017	AKD	Ugrađena podrška za vizualni dio potpisa na PDF dokumentu
2.1	1.7.2018	AKD	Proširena podrška PADES formatima
2.2	14.2.2019	AKD	Nadopunjeni primjeri poziva ePotpis WS Izmjene na vizualu potpisa: - Veličina i pozicioniranje vizuala - Proširenje mogućnošću upisa teksta kojeg šalje e-Usluga - Podrška za .NET Core u PAdES-u
2.3	8.7.2019	AKD	Proširen prostor za tekstualnu poruku u vizualu potpisa - 3 zasebna reda po 60 znakova
2.4	16.7.2019	AKD	Ugrađena podrška za pozicioniranje lokacije vizuala potpisa
3.0	28.7.2019	AKD	Implementacija PAdES kao lokalnog web servisa Dodana podrška za Batch potpis sa udaljenim certifikatima Promjena adresa ePotpis Web servisa
3.1	1.7.2020	AKD	Dodana podrška za PAdES T format. Unaprjeđenja u radu sa PDF formatima.
3.2	30.06.2021	AKD	Promijenjeni URL-ovi sa *id.hr* na *certilia.com*
4.0	22.12.2021	AKD	Revizija dokumenta. Ispravljeni primjeri za PAdES pre/post sign. Dodani novi primjeri. Ažurirano poglavlje PAdES Web API. Brisana ovjera dokumneta. Promijenjena struktura i formatiranje dokumenta. Dodani sadržaji vezano za PADES API DLL komponentu.
4.0.1	25.03.2022.	AKD	Dodan AdES Web API sadržaj i popis grešaka.
4.0.2	26.05.2022.	AKD	Manje ispravke grešaka u tekstu.
4.0.3	01.02.2023	AKD	Dodai oib i mobileSign parametri u primjeru poziva u točci 5.2.2.1.1
4.0.4	15.03.2023	AKD	Dodan country parametar u primjeru poziva u točci 5.2.2.1.1

4.0.5	15.04.2023	AKD	Ukinuta podrška za PAdES dll komponentu
4.0.6	06.07.2023.	AKD	Dodan parametar mimetype u točci 5.2.1.1.1
4.0.7	12.12.2023.	AKD	Dodan documentName opcionalni parametar u primjeru poziva u točci 5.3.5.3 Dodani CertiliaCA url-ovi u točci 3.5.1 Ispravljen prilog C (Polje Izdavatelj certifikata se ne koristi).
4.0.8	18.03.2024.	AKD	Ispravci dokumenta vezano za prestanak korištenja dll verzije PAdES API biblioteke. Dodane definicije. Dorađeno AdES poglavlje sa dodatnim pojašnjenjima. Manji ispravci.
4.0.9	28.03.2024.	AKD	Dodan parameter signatureType i expireAt (5.2.1) Dodana metoda za izračun lokacija vizuala za proizvoljnu veličinu stranice u 6.1 Prilog A.
4.0.10	27.08.2024.	AKD	Napravljeni manji ispravci. Dodatna pojašnjenja. Ažuriran url za servis za izradu vremenskog žiga.
4.0.11	03.03.2025.	AKD	Novi AdES Web API URL-ovi.
4.0.12	05.12.2025.	AKD	Slanje JSON objekta u slučaju kada korisnik odbije potpisivanje putem mobilne aplikacije.
4.0.13.	19.03.2026.	AKD	Ispravci naziva parametara za lokaciju vizuala (PadES). Izbačen popis AdES grešaka, dostupan url za download.
4.0.14.	29.06.2026.	AKD	Napravljeni manji ispravci grešaka u tekstu i formatiranju. Dodana mogućnosti korištenja dodatnog vizuala (id='small') koji je dimenzijama manji i sadrži manji set podataka od standardnog vizuala (PadES). Ažurirana odgovarajuća poglavlja i prilozi sa dodatnim opisima, parametrima i primjerima korištenja.

1 Uvod

Ovaj dokument definira tehničke preduvjete za integraciju sustava pružatelja e-Usluge i AKD ePotpis rješenja za potrebe izrade kvalificiranog elektroničkog potpisa digitalnog dokumenta koristeći elektroničku osobnu iskaznicu.

Svrha dokumenta je specificirati zahtjeve za razmjenu podataka u sklopu integracije s ciljem osiguranja sigurne razmjene i jedinstvene identifikacije korisnika. Dokument je izrađen temeljem dosadašnje najbolje prakse koja osigurava sigurnu razmjenu podataka i zaštitu prijenosa.

Pojmovi:

- e-Usluga – programsko rješenje koje želi implementirati izradu kvalificiranog elektroničkog potpisa
- Pružatelj e-Usluge – pravna ili fizička osoba koja putem e-Usluge želi izrađivati kvalificirani elektronički potpis
- e-Potpis – AKD-ovo integracijsko programsko rješenje koje omogućava implementaciju funkcionalnosti izrade kvalificiranog elektroničkog potpisa iz e-Usluge
- eOI (elektronička osobna iskaznica) ili KID kartica – sredstvo za izradu kvalificiranog elektroničkog potpisa (QSCD) uređaj sukladan EU 910/2014 eIDAS direktivi koji sadrži kvalificirani potpisni certifikat izdan od ovjerovitelja HRIDCA ili KIDCA
- System ID – Identifikacijska oznaka Pružatelja e-Usluge dodijeljena od strane AKD-a za potrebe integracije s AKD e-Potpisom
- Service ID – Identifikacijska oznaka e-Usluge dodijeljena od strane AKD-a za potrebe integracije s AKD e-Potpisom
- Document ID – identifikacijska oznaka dokumenta za kojega se izrađuje kvalificirani elektronički potpis
- PAdES (PDF Advanced Electronic Signatures) – format za izradu naprednog elektroničkog potpisa
- Jednokratni token – identifikator komunikacije sa ePotpis sustavom
- Verifikacijski kod – kod za provjeru valjanosti potpisa
- Level B-B ili B – nivo ili razina potpisa B (vidi **Error! Reference source not found.**.1)
- Level B-T ili T – nivo ili razina potpisa T (vidi **Error! Reference source not found.**.1)
- Level B-LT ili LT – nivo ili razina potpisa LT (vidi **Error! Reference source not found.**.1)
- Level B-LTA ili LTA – nivo ili razina potpisa LTA (vidi **Error! Reference source not found.**.1)
- TSA ili TimeStamp servis – servis za ugradnju vremenskog žiga
- Certificate chain – svi CA certifikati potrebni za provjeru korisničkog certifikata

1.1 Reference

1. https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/doc/dss-documentation.html

2 Podaci pružatelja e-Usluge

Dokument sa popunjenim podacima iz ovog poglavlja je potrebno poslati na email adresu esign@certilia.com

2.1 Naziv pružatelja e-Usluga (npr. Organizacija A)

_____

2.2 Naziv e-Usluge (npr. E-Zahtjev)

_____

2.3 Nazivi dokumenata (npr. Zahtjev za upis u...)

1. _____
2. _____
3. _____
4. _____

2.4 Bazni URL klijenta

**npr: https://usluga.hr/eSign*

https:// _____

[TEST]
https://_____

2.5 URL na kojem se nalazi potpis pdf-a sa klijentske strane

**Adresa na strani e-Usluge iz koraka 6.b. u dijagramu 1., npr: https://usluga.hr/eSign/SignPdf*

https://_____

[TEST]

https://_____

2.6 URL na koji se preusmjeruje nakon uspješnog potpisa

**Adresa na strani e-Usluge iz koraka 6.c. u dijagramu 1., npr: https://usluga.hr/eSign/Success/?token=*

https://_____

[TEST]

https://_____

2.7 URL na koji se preusmjeruje kad dođe do greške

**Adresa na strani e-Usluge iz koraka 6.c. u dijagramu 1., npr: https://usluga.hr/eSign/Error/?token =*

https://_____

[TEST]

https://_____

2.8 (Opcija) Bazni URL na kojem usluga skladišti potpisane dokumente za potrebe dohvata kod verifikacije

**npr.: 'https://usluga.hr/docs/'*

https://_____

** Adresa na strani e-Usluge putem koje krajnji korisnik može dohvatiti izvornik elektronički potpisanog dokumenta.*

***NAPOMENA**: naziv datoteke treba biti u formatu "verificationCode.pdf" (npr. https://usluga.hr/docs/5a4df4daee6bec19fcaee82e.pdf)*

[TEST]

https://_____

2.9 Adrese servera e-usluge

IP adresa/e: _____

2.10 Osoba za administraciju putem Certilia Developer portala

OIB osobe: _____

*Upisuje se OIB osobe koja će prijavom na https://developer.certilia.com administrirati vašu uslugu. Administracija uključuje mogućnost promjene podataka iz točaka 2.3 do 2.9 , uvid u statistike korištenja i prekid usluge.

3 Preduvjeti za integraciju

3.1 Mrežni preduvjeti

- Mrežna povezanost pružatelja usluge i AKD ePotpis servisa za potrebe komunikacije web servisima
- Valjan serverski certifikat za potrebe zaštite kanala između pružatelja e-Usluge i ePotpis servisa
- Dostupnost sa klijentskog računala AKD servisa navedenih u poglavlju 3.5 URL AKD servisa za provjeru statusa certifikata i TSA
- Dostupna mrežna povezanost sa svih servera pružatelja e-Usluga na kojima se nalaze ePotpis komponente, prema [TEST]esign.test.certilia.com i esign.certilia.com
- Omogućene zadnje verzije TLS-a na klijentskim računalima

3.2 Identifikacijski podaci za korištenje ePotpis rješenja

- Od strane AKD-a izdan ID sustava pružatelja e-Usluge koji je registriran u ePotpis servisu
- Od strane AKD-a izdan ID usluge pružatelja e-Usluge koji je registriran u ePotpis servisu
- Od strane AKD-a izdan ID dokumenta pružatelja e-Usluge koji je registriran u ePotpis servisu

3.3 Potpisni certifikati

Potpisni certifikat izdavatelja AKD d.o.o. najmanje na jednom od navedenih medija :

a. Potpisni certifikat na eOI iskaznici (elektronička osobna iskaznica RH) kartici
b. Potpisni certifikat na KID kartici
c. Potpisni certifikat za kreiranje elektroničkog potpisa na infrastrukturi pouzdanog pružatelja usluge (cloud certifikat, certifikat u oblaku)

3.4 Programski paket za rad s pametnom karticom - Middleware

Za eOI iskaznicu na računalima korisnika potrebno je instalirati zadnje dostupne verzije eID Middleware. Dostupno za preuzimanje na https://eid.hr/.

Za KID karticu na računalima korisnika potrebno je instalirati zadnje dostupne verzije Certilia Middleware. Dostupno za preuzimanje na https://www.certilia.com/.

Napomena: Preporuča se upotreba zadnje dostupnih verzija zbog periodičkog obnavljanja klijentskih certifikata uključenih u Middleware pakete.

3.5 URL AKD servisa za provjeru statusa certifikata i TSA

URL su kodirani unutar samog certifikata te se preporuča koristiti iste obradom certifikata.

Moguće su i druge vrijednosti ovisno o promjenama u izdavanju – vidi pravila i postupke certificiranja (CP, CPS) na www.certilia.com i www.eid.hr.

Primjeri vrijednosti za dani u nastavku.

3.5.1 CertiliaCA

A. [TEST]

1. URL= https://crl.test.certilia.com/certilia.crl
2. URL= https://ocsp.test.certilia.com/certilia

   ROOT
3. URL=http://crl1test.id.hr/testakdcaroot.crl
4. URL=http://crl2test.id.hr/testakdcaroot.crl
5. URL=http://ocsptest.id.hr/testakdcaroot

B. [PROD]

6. URL= https://crl.certilia.com/certilia.crl
7. URL= https://ocsp.certilia.com

   ROOT
8. URL=http://crl1.id.hr/akdcaroot.crl
9. URL=http://crl2.id.hr/akdcaroot.crl
10. URL=http://ocsp.id.hr/akdcaroot

3.5.2 KIDCA

A. [TEST]

1. URL=http://crl1test.id.hr/testkidca.crl
2. URL=http://crl2test.id.hr/testkidca.crl
3. URL=http://ocsp-testkidca.id.hr/testkidca

   ROOT
4. URL=http://crl1test.id.hr/testakdcaroot.crl
5. URL=http://crl2test.id.hr/testakdcaroot.crl
6. URL=http://ocsptest.id.hr/testakdcaroot

B. [PROD]

7. URL=http://crl1.id.hr/kidca.crl
8. URL=http://crl2.id.hr/kidca.crl
9. URL=http://ocsp-kidca.id.hr/kidca

   ROOT
10. URL=http://crl1.id.hr/akdcaroot.crl
11. URL=http://crl2.id.hr/akdcaroot.crl
12. URL=http://ocsp.id.hr/akdcaroot

3.5.3 HRIDCA

A. [TEST]

1. URL=http://crl1test.eoi.hr/testhridca.crl
2. URL=http://crl2test.eoi.hr/testhridca.crl
3. URL=http://ocsp-testhridca.eoi.hr/testhridca

   ROOT
4. URL=http://crl1test.eoi.hr/testakdcaroot.crl
5. URL=http://crl2test.eoi.hr/testakdcaroot.crl
6. URL=http://ocsptest.eoi.hr/testakdcaroot

B. [PROD]

13. URL=http://crl1.eid.hr/hridca.crl
14. URL=http://crl2.eid.hr/hridca.crl
15. URL=http://ocsp-hridca.eid.hr/hridca

    ROOT
16. URL=http://crl1.eid.hr/akdcaroot.crl
17. URL=http://crl2.eid.hr/akdcaroot.crl

    URL=http://ocsp.eid.hr/akdcaroot

3.5.4 TSA

[TEST] : https://tsa.test.certilia.com/qts za [TEST]

[PROD] : https://tsa.certilia.com/qts za [PROD]

4 Opis ePotpis rješenja

4.1 Komponente AKD ePotpis rješenja

Komponente AKD ePotpis rješenja su:

4.1.1 ePotpis

- Web servis za potpisivanje: https://esign.certilia.com/epotpis
- Web aplikacija za provjeru: https://esign.certilia.com/provjera

4.1.2 PAdES/XAdES web api

a. Generiranje hash-a iz PDF/XML dokumenta

b. Ugradnja potpisanog hash-a u PDF/XML dokument

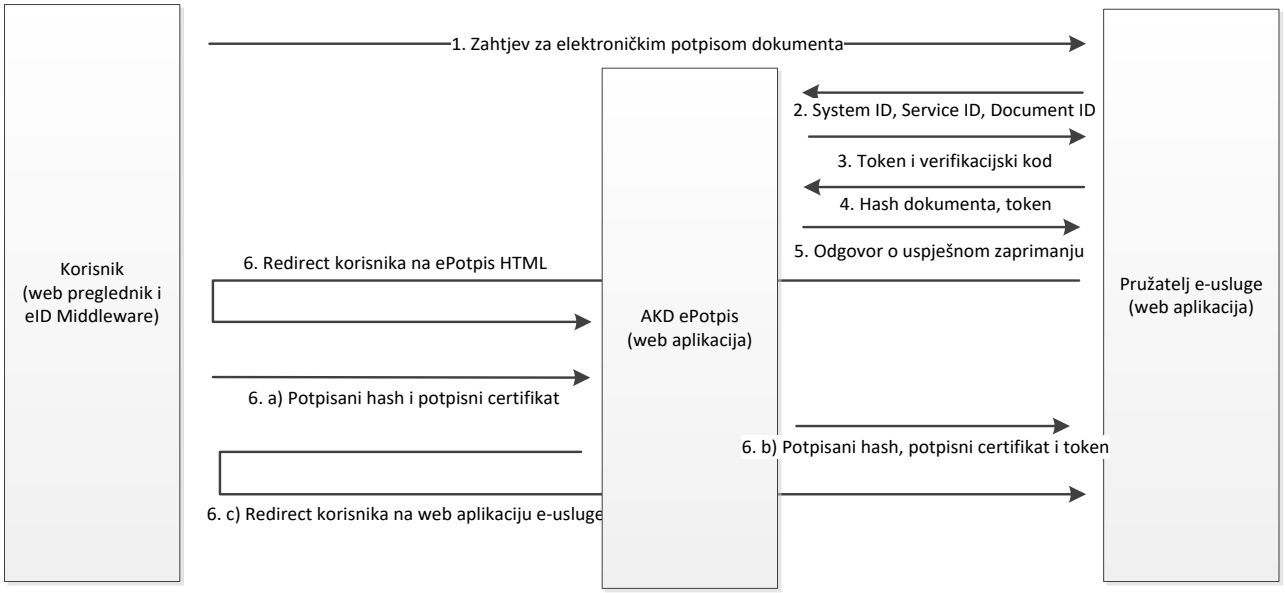
4.2 Funkcionalnosti ePotpis rješenja

Osnovne funkcionalnosti AKD ePotpis rješenja su:

1. Generiranje hash-a dokumenta
2. Potpis dokumenta potpisnim certifikatom (certifikat na kartici, certifikat u oblaku)
3. Ugradnja potpisanog hash-a u konačni dokument
4. Ugradnja vizualnog prikaza podataka o kreiranom kvalificiranom potpisu u konačni dokument (Opcionalno)
5. Mogućnost provjere potpisa na sustavu ePotpis (Opcionalno, preduvjet točka 4.)

4.3 Dijagram toka komunikacije komponenti

Dijagram toka opisuje tijek i redoslijed razmjene podataka između pružatelja e-usluge i AKD ePotpis servisa (Slika 1).



Slika 1: Dijagram toka

1. U trenutku kada korisnik e-Usluge želi potpisati dokument(e) kvalificiranim elektroničkim potpisom, on potvrđuje namjeru elektroničkog potpisivanja svojeg zahtjeva klikom na gumb unutar e-Usluge.
2. e-Usluga poziva web servis AKD ePotpis i šalje *System ID*, *Service ID* i *Document ID, te broj dokumenata*. (Primjer 5.2.1)
3. Temeljem primljenih parametara ePotpis generira jedinstveni token i verifikacijski kod za svaki dokument, kao odgovor.
4. e-Usluga iz PDF/XML dokumenta putem PAdES/XAdES web API-a (0) generira hash nepotpisanog/ih PDF/XML dokumenta. e-Usluga dostavlja hash i token ePotpis servisu (5.2.2).
5. U slučaju uspješnog odgovora AKD ePotpis servisa, e-Usluga treba preusmjeriti korisnika na stranicu koja je udomljena na serverima AKD-a. Poziv ePotpis web stranice uključuje i token dobiven od AKD ePotpis servisa u ranijem koraku (Slika 2) (5.2.3).



Slika 2: Certilia ePotpis web

6. Korisnik će putem ove stranice elektronički potpisati hash dokumenta koje mu je e-Usluga prethodno stavila na uvid.
7. U slučaju neuspjeha, AKD ePotpis će ovisno o tipu greške ponuditi korisniku ponovni pokušaj ili prikazati obavijest da trenutno nije moguće izvršiti elektroničko potpisivanje dokumenta.
8. Nakon uspješnog potpisivanja hash(eva):
    a. informacija o elektronički potpisanom hashu dokumenta, te informacija o potpisnom certifikatu koji je obavio elektroničko potpisivanje, kao i drugi potrebni podaci se pohranjuju u bazu ePotpis servisa AKD-a
    b. informacija o elektronički potpisanom hashu(evima) zahtjeva prosljeđuje se e-Usluzi pozivanjem za to predviđenog web servisa koji je izložen od strane e-Usluge iz točke 2.5. (5.2.4)
    Potpisani(e) hash(eve) e-Usluga ugrađuje u PDF/XML dokument putem PAdES/XAdES API-a.
    c. korisnik se sa ePotpis web stranice putem koje je obavio elektroničko potpisivanje preusmjerava na za to predviđene stranice e-Usluge iz točke 2.6. (**Error! Reference s ource not found.**)

Pružatelj e-Usluge može omogućiti dohvaćanje elektronički potpisanog dokumenta, u svrhu verifikacije putem ePotpis web aplikacija za provjeru elektronički potpisanih dokumenata.

9. PAdES/XAdES web API-a obavlja ugradnju potpisanog(ih) hash(eva) po PAdES part 3 i XAdES, odnosno eIDAS nivo ili razina B, T, LT ili LTA standardu (vidi 1.1).

5 Integracijske komponente

Integracija sustava e-Usluge s ePotpis servisom se obavlja u četiri točke:

1. Razmjena podataka za potpis (koraci 2. i 3. dijagrama toka)
2. Preusmjeravanje korisnika na ePotpis (korak 6. dijagrama toka)
3. Vraćanje potpisanih podataka (korak 6.b dijagrama toka)
4. Preusmjeravanje korisnika, nakon potpisa, na stranu pozivatelja (korak 6.c dijagrama toka)

5.1 Definicije

5.1.1 Potpis

Elektronički potpis (potpis, „sign“) – kvalificirani eIDAS elektronički potpis (pdf/xml). Može biti u privatne ili poslovne svrhe. Potpisnik je fizička osoba. U certifikatu se obavezno nalaze podaci fizičke osobe (npr. certifikati na osobnoj iskaznici RH (eOI) ili udaljeni certifikati izdani temeljem osobne iskaznice) a ukoliko se radi o poslovnom certifikatu u istom se dodatno nalaze i podaci organizacije (pravna osoba) povezane s fizičkom osobom (npr. Certilia/KID poslovni certifikati, udaljeni ili na kartici).

Kada se koristi ugradnja vizuala kod potpisa u privatne svrhe, **obavezno** se prosljeđuju podaci fizičke osobe u parametru **personNaturalData** (vidi parametre).

Kada se koristi ugradnja vizuala kod potpisa u privatne svrhe, **obavezno** se prosljeđuju podaci fizičke osobe u parametru **personNaturalData** (vidi parametre).

5.1.2 Pečat

Elektronički pečat (pečat,“seal“) – kvalificirani eIDAS elektronički pečat (pdf/xml) u poslovne svrhe. Potpsinik je odgovorna osoba u ime organizacije – u certifikatu se nalaze podaci pravne osobe.
Kada se koristi ugradnja vizuala, **obavezno** se prosljeđuju podaci pravne osobe u parametru **personLegalData** (vidi parametre).

5.1.3 Token

Jednokratan, jedinstveni token koji se dobiva prilikom poziva ePotpisnog servera opisanog u točki 4.1. zasniva se na JSON Web Token standardu. Opis formata spomenutog standarda kao i pripadajuće biblioteke za implementaciju standarda mogu se preuzeti sa https://jwt.io/ linka. Token se sastoji od tri dijela:

- Header – tip tokena i hashing algoritam koji se koristi (Base64 kodirano)
- Payload – podaci o trenutnoj sesiji/korisniku (Base64 kodirano)

- Signature – hash prethodna dva dijela i ključa kojim je osigurana autentičnost te integritet podataka

Token služi kao jedinstveni i jednoznačni identifikator transakcije (potpisa).

Njegov sadržaj bitan je za korisnika prilikom kontaktiranja korisničke podrške. Radi bržeg dijagnosticiranja problema vrijednost tokena potrebno je slati prilikom prijave kao tekst (ne kao snimak zaslona).

5.1.4 Verifikacijski kod

Jednokratan, jedinstveni UID koji se dobiva prilikom poziva ePotpisnog servera opisanog u točki 4.1.

Token služi kao jedinstveni i jednoznačni identifikator pojedinog dokumenta odnosno potpisa unutar transakcije. Verifikacijski kod ugrađen je u podatke potpisa, element je vizuala kao tekst i unutar QR koda.

Njegov sadržaj bitan je za korisnika prilikom kontaktiranja korisničke podrške. Radi bržeg dijagnosticiranja problema vrijednost verifikacijskog koda potrebno je slati prilikom prijave kao tekst (ne kao snimak zaslona).

5.1.5 Vizual

Vizual je grafički element koji se ugrađuje (opcionalno) prilikom izračuna hasha. Elementi vizuala prikazani su u prilogu Prilog B – Elementi standardnog vizuala. Veličina i izgled vizuala su unaprijed zadani te nisu moguće proizvoljne promjene grafičkog izgleda. Moguće lokacije unutar A4 stranice prikazane su u prilogu Prilog A – Lokacije vizualnog elementa unutar A4 stranice.

Korištenje (prikaz) vizuala odnosno nekorištenje istog prilikom ugradnje potpisa određeno je korištenjem parametra addVisualData i opcionalnih parametara (vidjeti opis parametara i primjere).

Napomena: kod XAdES servisa termin vizual se odnosi na dodavanje komentara u xml sa istim podacima koji se koriste u vizualu (osim QR koda) a prema dostupnim parametrima XAdES servisa.

5.1.6 PersonNaturalData

Podaci fizičke osobe (OIB, Ime i prezime, država osobe) koji se nalaze u certifikatu. Kod opcije ugradnje vizuala obavezno se šalju navedeni podaci u POST (PreSign) pozivu prema servisu radi provjere prilikom ugradnje potpisne vrijednost sa podacima upisanim u certifikat. Na ovaj način se osigurava da je potpis kreirala osoba čiji podaci su prikazani u elementima vizuala.

Važno: *Podaci se šalju na servis samo ako se koristi opcija ugradnje vizuala te prilikom kreiranja potpisa.*

5.1.7 PersonLegalData

Podaci pravne osobe (VAT tj. porezni broj/OIB , naziv organizacije, država organizacije, opcionalno naziv pečata) koji se nalaze u certifikatu. Kod opcije ugradnje vizuala obavezno se šalju navedeni podaci u POST (PreSign) pozivu prema servisu radi provjere prilikom ugradnje potpisne vrijednost sa podacima upisanim u certifikat. Na ovaj način se osigurava da je potpis kreiran u ime pravne osoba čiji podaci su prikazani u elementima vizuala.

Važno: *Podaci se šalju na servis samo ako se koristi opcija ugradnje vizuala i to: opcionalno prilikom potpisa (ako fizička osoba kreira potpis u poslovne svrhe), obavezno prilikom krieranja pečata.*

5.2 ePotpis

5.2.1 Zaprimanje inicijalnih podataka za potpis

Sustav e-Usluge šalje System ID, Service ID, Document ID kao servisne parametre, te broj dokumenata[1] koji se namjerava potpisati. Kao odgovor e-Usluga dobiva jedinstveni, jednokratni token ograničenog vijeka trajanja te verifikacijski kod za svaki dokument.

Protokol: HTTPS

URL:
[PROD]: https://esign.certilia.com/api/v2/epotpis
[TEST] : https://esign.test.certilia.com/api/v2/epotpis

HTTP Metoda: POST

Sigurnost: SSL(TLS1.2, TLS1.3)

Opis značenja parametara:
systemId (dodijeljen od strane AKD-a za svaki sustav pozivatelja)
serviceId (dodijeljen od strane AKD-a za svaku uslugu sustava pozivatelja)
documentId (dodijeljen od strane AKD-a za svaki dokument sustava pozivatelja)
numOfDocs - Broj dokumenata za potpisivanje
mimetype – tip dokumenta („xml“ ili „pdf“), ako se ne posalje default je „pdf“
signatureType – označava tip certifikata, poptis ili pečat, te se na temelju tog parametra krisniku prikazuju certifikati, ako nije poslano prikazju mu se svi certifikati

5.2.1.1 Primjer 1a – Zaprimanje inicijalnih podataka kod potpisivanja jednog dokumenta

5.2.1.1.1 Upit

```
JSON DATA:
{
        "authData": {
                "systemId": "100",
                "serviceId": "500",
                "documentId": "600"
        },
        "signingData": {
                "numOfDocs": "1",
                "mimetype": "xml", // potreban ako je dokument XML, ako se ne pošalje smatra se da je dokument PDF
                "signatureType": "sign" // „sign“ ako je Potpis, „seal“ ako je pečat,
        }
}
```

[1] Potpisivanje više dokumenata je moguće isključivo certifikatima za udaljeni potpis. Više informacija o certifikatima za udaljeno potpisivanje možete pronaći na poveznici https://www.certilia.com/certilia-mobileid/.

5.2.1.1.2 Odgovor

```
JSON DATA:
{
        "authDataResponse": {
                "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0cmFjZUlkIjoiMWJmNjdkYmEtNTVmNS00MjdjLWJiMzEtODIyMjRjOWZmZDlkIiwiaWF0IjoxNTY0MzI2MjkxLCJleHAiOjE1NjQzMjk4OTF9.-oUig1hN-xEhU7KcG4s4yZZ1qkI-yJXn40T3DiVuFjY",
                "verificationCodes": [
                        "879fd6ec-6c60-4932-bd92-752cae326017"
                ],
                "expireAt": ''2024-03-28T08:35:07.000Z'' // vrijeme trajanja transakcije
        }
}
```

5.2.1.1.3 Odgovor u slučaju GREŠKE

```
{
  "error": {
    "status": 400,
    "id": "f8663cee-1f0e-4cfc-8bac-fdfdfa664d81",
    "message": "Missing required parameter",
    "code": null
  }
}

 Ili:

{

  "error": {
    "status": 400,
    "id": "f8663cee-1f0e-4cfc-8bac-fdfdfa664d81",
    "message": "Invalid auth data",
    "code": null
  }
}
```

I slično.

5.2.1.2 Primjer 1b – Zaprimanje inicijalnih podataka kod potpisivanja više dokumenta

5.2.1.2.1 Upit

```
JSON DATA:
{
        "authData": {
                "systemId": "100",
                "serviceId": "500",
                "documentId": "600"
        },
        "signingData": {
                "numOfDocs": "5"
        }
}
```

5.2.1.2.2 Odgovor

```
JSON DATA:
{
        "authDataResponse": {
                "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0cmFjZUlkIjoiMDM3Mjc2MmQtOTY1My00NTBmLTk0MTUtZTg
0MjMzZGJjMmJjIiwiaWF0IjoxNTY0MzI2MzQzLCJleHAiOjE1NjQzMjk5NDN9.15GME1onQa2ZhhbxIsu7n4x-
DPPmnfMKcvPwxYqo40k",
                "verificationCodes": [
                        "9f657817-9739-4546-8bbb-02c947bf1bfd",
                        "dd29565b-9d95-4867-87f1-a1d4fd071dd2",
                        "1a646d93-8fa2-455a-bbba-ba771c5e0fd6",
                        "6e88e918-d25f-4428-88ff-af97920d2464",
                        "5eacfdc8-a176-4c1e-b2c4-52ee6c6295ba"
                ]
        }
}
```

5.2.1.2.3 Odgovor u slučaju greške

```
{
   "error": {
      "status": 400,
      "id": "f8663cee-1f0e-4cfc-8bac-fdfdfa664d81",
      "message": "Missing required parametar",
      "code": null
   }
}

 Ili:

{
   "error": {
      "status": 400,
```

```
    "id": "f8663cee-1f0e-4cfc-8bac-fdfdfa664d81",
    "message": "Invalid auth data",
    "code": null
  }
}
```


I slično.

5.2.2 Zaprimanje hash-a dokumenta za potpis

Sustav e-Usluge šalje hash dokumenta prema ePotpis servisu koji će u idućem koraku biti proslijeđen korisniku na potpis.

Korištenjem opisanih opcionalnih parametara e-usluga može preskočiti korisnički odabir načina potpisivanja i koristiti direktno način potpisivanja „Nastavi na mobitelu“.

Napomena: *Za „nastavi na mobitelu“ korisnik koji potpisuje treba imati izdan važeći udaljeni certifikat i aktivnu Certilia mobilnu aplikaciju.*

Protokol: HTTPS

URL:
[PROD] https://esign.certilia.com/api/v2/epotpis/hash
[TEST] https://esign.test.certilia.com /api/v2/epotpis/hash
** Varijabla token sadrži vrijednost dobivenu u prethodnom koraku.*

HTTP Metoda: PATCH

Sigurnost: SSL(TLS1.2, TLS1.3)

5.2.2.1 Primjer 2 – Zaprimanje hash-a za jedan dokument

5.2.2.1.1 *Upit*

```
JSON DATA:
{
	"authData": {
		"token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0cmFjZUlkIjoiODE5ZWM2ZjgtZTgyNi00NjQxLTg5YTItNWI4ZGZh
NjgxMmQ5IiwiaWF0IjoxNTY0MzI3MzY0LCJleHAiOjE1NjQzMzA5NjR9.PCAUACMWVBEf0TNvBSWTr9bQzNF
YixO-V8O6dnHqZJg"
	},
	"signingData": {
		"documents": [
			{
				"hash":
"3959422b38556f6c79526b567464786d3959422b38556f6c79526b567464786d",
				"verificationCode": "4cd9e6fb-676e-451b-a6a6-6a09a4e94251"
			}
		],
		"oib":"oib potpisnika",  // obavezan samo ako je mobileSign === true
		"country":"Drzava koja je izdala identifikacijski broj, npr. 'HR'",  // obavezan samo ako je
mobileSign === true
		"mobileSign": true ili false,  // opcionalan parametar; ako je true, potpisuje se isključivo
putem Certilia mobilne aplikacije

	}

}
```

5.2.2.1.2 Odgovor

```
JSON DATA:
{
	"authDataResponse": {
		"token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0cmFjZUlkIjoiODE5ZWM2ZjgtZTgyNi00NjQxLTg5YTItNWI4ZGZhNjgxMmQ5IiwiaWF0IjoxNTY0MzI3MzY0LCJleHAiOjE1NjQzMzA5NjR9.PCAUACMWVBEf0TNvBSWTr9bQzNFYixO-V8O6dnHqZJg"
	},
	"signingDataResponse": {
		"success": true
	}
}
```

5.2.2.1.3 Odgovor u slučaju greške

```
{
	"error": {
		"status": 400,
		"id": "819ec6f8-e826-4641-89a2-5b8dfa6812d9",
		"message": "Parameter [hash] must be 64 character hexadecimal string string. [Details:
hash => 3959422b38556f6c79526b567464786d3959422b38556f6c79526b567464786]",
		"code": null
	}
}
```

5.2.3 Preusmjeravanje korisnika na potpisno rješenje

Personalizacija HTML stranice za elektroničko potpisivanje se vrši na temelju jedinstvenog tokena.

Protokol: HTTPS

URL:
[PROD]: https://esign.certilia.com/epotpis/?token=$token
[TEST] : https://esign.test.certilia.com/epotpis/?token=$token

Parametar: token

HTTP Metoda: GET

Sigurnost: SSL(TLS1.2, TLS1.3)

Odgovor sustava:

- HTTP 200 – uspješna akcija

Alternativni odgovor:

- HTTP 400 – greška

5.2.4 Vraćanje potpisanih podataka

Informacija o potpisan hashu(evima), pripadajućem verifikacijskom kodu i potpisnom certifikatu dostaviti će se na stranu e-Usluge pozivom web servisa. REST web servis mora biti izložen (dostupan) sa strane e-Usluge, na adresi iz točke 2.5.

AKD će, nakon što potpisani hash zapiše u svoj sustav (korak 6.a dijagrama toka), pozvati spomenuti web servis i proslijediti mu informaciju o elektronički potpisanom hashu(evima) dokumenta i potpisnom certifikatu koji je obavio potpisivanje. Tom prilikom, AKD će e-Usluzi unutar poziva web servisa ponovno navesti i prethodno razmijenjen token.

Protokol: HTTPS

URL: URL e-Usluge iz točke 2.5.
[TEST] : URL e-Usluge iz točke 2.5.

HTTP Metoda: POST

Sigurnost: SSL(TLS1.2, TLS1.3)

5.2.4.1 Primjer 3 – Vraćanje potpisanih podataka

5.2.4.1.1 Upit

```
JSON DATA:
{
  "authData": {
    "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0cmFjZUlkIjoiODE5ZWM2ZjgtZTgyNi00NjQxLTg5YTItNWI4ZGZh
NjgxMmQ5IiwiaWF0IjoxNTY0MzI3MzY0LCJleHAiOjE1NjQzMzA5NjR9.PCAUACMWVBEf0TNvBSWTr9bQzNF
YixO-V8O6dnHqZJg "
  },
  "signingData": {
    "userCertificate": "SDFSDFGSDSFDFSDWW…",
    "documents": [
      {
        "hash": "pdf1base64",
        "signedHash": "0011AA...",
        "verificationCode": "randomnumber"
      },
      {
        "hash": "pdf1base642",
        "signedHash": "0011AA...",
        "verificationCode": "randomnumber2"
      }
    ]
  }
}
```

5.2.4.1.2 Odgovor

```
HTTP code: 201

JSON DATA:
{
  "signingDataResponse": {
    "status": "201"
  }
}
```

5.2.4.1.3 Odgovor u slučaju greške

```
HTTP code: 400

{
  "error": {
    "status": "400",
    "code": "VAŠ ID GREŠKE",
    "title":"Opis greške"
  }
}
```

5.2.4.2 Korisnik je odbio potpisivanje putem mobilne aplikacija

U slučaju kada korisnik odbije potpisivanje putem mobilne aplikacija, na URL za ugradnju šalje se JSON objekt

Protokol: HTTPS

URL: URL e-Usluge iz točke 2.5.
[TEST] : URL e-Usluge iz točke 2.5.

HTTP Metoda: POST

Sigurnost: SSL(TLS1.2, TLS1.3)

```
JSON DATA:

{
  "error": {
    "token": "token transakcije",
    "message": "Korisnik je odbio potpisivanje transakcije putem mobilne aplikacije",
    "errorId":"id greške"
  }
}
```

5.3 AdES (PAdES / XAdES) WEB API

AdES WEB API je servis koja služi za generiranje hash-a i ugradnju potpisanog hash-a u PDF ili XML dokument.

AdES je dostupan isključivo kao REST Web Servis. Servis koristi isključivo AKD [TEST] i [PROD] servise za ugradnju vremenskog žiga (timestamp servis).

Podržana je ugradnja potpisa nivoa ili razine:

a. B-B

b. B-T

c. B-LT

d. B-LTA

Za razine potpisa B-T, B-LT i B-LTA nužno je osigurati pristupne podatke za ugradnju vremenskog žiga AKD TSA servisa.

Ugradnje je sukladna ETSI_EN_319_132 XAdES standardima (dostupno na npr. https://en.wikipedia.org/wiki/XAdES.

5.3.1 Tehnički preduvjeti

Vlasnik e-Usluge osim uvjeta navedenih u točki 3 Preduvjeti za integraciju mora osigurati preduvjete prema točkama u nastavku.

5.3.1.1 Postavke sustava

Smjernice za vlasnika e-Usluge:

- Osigurati SSL postavke na računalu na kojem se poziva servis. Podržane su najnovije verzije TLS*.
- Za pojačani rad komponente u okolinama sa većim brojem dokumenta odnosno sa dokumentima koji su veličinom više od nekoliko MB ili desetak MB potrebno je osigurati više radne memorije i diskovnog prostora te odgovarajuću jaču procesnu snagu.

5.3.1.2 Podaci za AKD TimeStamp servis

Vlasnik e-Usluge je odgovoran za pribavljanje pristupnih podataka za AKD TimeStamp servis ukoliko želi kreirati potpise razine T, LT i LTA.

Podaci za pristup [TEST] i/ili [PROD] AKD TimeStamp servisu izdaju se temeljem Zahtjeva za pristup servisu usluge za izdavanje kvalificiranog vremenskog žiga. Zahtjev je dostupan za preuzimanje na https://www.certilia.com.

Kod izdavanja podataka za [TEST] servis potrebno je naznačiti na zahtjevu da se radi o [TEST] servisu.

URL servisa:

[TEST] : https://tsa.test.certilia.com/qts za [TEST]

[PROD] : https://tsa.certilia.com/qts za [PROD]

5.3.2 Osnovne funkcionalnosti

- Generiranje hash-a PDF / XML dokumenta
- Ugradnja potpisanog hash-a u PDF / XML dokument
- Automatska ugradnja vremenskog žiga za razine T, LT i LTA
- Opcionalna ugradnja vizualnog elementa potpisa

5.3.3 Ograničenja i preporuke za korištenje servisa

Broj dokumenta koji se može poslati u pojedinom pozivu prema servicu nije ograničen (parametar **documents[]**).

Na sustavu je primjenjeno ograničenje na promet (payload). Ograničenje po pojedinom pozivu postavljeno je na cca 35MB. Ostale postavke sustava su sukladne industrijskim standardima (npr. broj poziva u minuti (rate limits) i sl.).

Važno: *Radi postizanja normalnih performansi ugradnje potpisa za sve korisnike servisa, preporuča se vlasnicima dokumenata da prilikom kreiranja istih obavezno koriste opcije koje omogućavaju kompaktnost dokumenata, odnosno smanjuju njihovu konačnu veličinu na prihvatljivu za korisnika i sustav kako bi se omogućile uobičajene performanse servisa. Npr. kod kreiranja pdf dokumenata smanjiti rezoluciju dokumenta i sadržaja na minimalnu moguću radi bržeg uploada/downloada i manipulacije istima.*

Napomena: *Sva ograničenja na sustavu su soft ograničenja, što znači da za korisnike koji odstupe od preporučenih vrijednosti prilikom korištenja sustava može doći do značajne degradacije performansi u operacijama koje zatraže od sustava. Npr. kod većh dokumenata, uobičajen je pad performansi u radu radi povećanja vremena trjanja operacija nad takvim dokumentima (duže vrijeme potrebno za upload/download i ostale operacije u kojima se manipulira dokumentima kroz komponente sustava).*

5.3.4 Napomene

5.3.4.1 Dodavanje prazne stranice (PAdES)

- U slučaju da PDF dokument koji se potpisuje ne sadrži elektroničke potpise komponenta dodaje dodatnu A4 (portrait) praznu stranicu kao zadnju stranicu dokumenta u slučajevima:
    - kada se potpisuje bez ugradnje vizualnog elementa
    - kada se potpisuje sa ugradnjom vizualnog elementa pri čemu su parametar int pageNumber = 0; i parametar int pageLocation = 0;
- Opcionalno je moguće parametrom odrediti da se umjesto dodavanja A4 portrait prazne stranice, dodaje stranica veličine i orijentacije zadnje stranice dokumenta koji se potpisuje.
    - Parametar koji je potrebno navesti u POST (5.3.5.1.1) metodi je:
        - "addBlankPageOptions": {
    - "blankPageOption": "ADD_AUTO_ON_NO_SIGNATURES"}
    - Npr. ako je zadnja stranica u dokumentu npr. A3 (landscape) dodati će se prazna stranica veličine A3 (landscape).
    - Navedeno vrijedi isključivo ako se ugrađuje vizual, ako se poptisivanje radi bez opcije ugradnje vizuala, dodati će se prazna A4 (portrait stranica).

5.3.4.2 Vizual (PAdES)

- Vizualni element je unaprijed zadan i nije moguća njegova promjena u smislu dizajna, veličine i sadržaja podržanih podatkovnih polja.
- Kada se koristi opcija ugradnje vizuala, servisu se obavezno dostavljaju podaci fizičke i/ili pravne osobe prilikom računanja HASH vrijednosti, u POST metodi (PreSign). Podaci fizičke osobe se dostavljaju u parametru personNaturalData a podaci pravne osobe u parametru personLegalData (vidi parametre).
    - personNaturalData – obavezno se dostavljaju parametri PIN i PINCountry, opcionalno nameSurname - za potpis koji kreira fizička osoba u privatne ili poslovne svrhe
    - personLegalData – obavezno se dostavljaju parametri VAT i VATCountry opcionalno name, sealName - za potpis koji kreira fizička osoba u poslovne svrhe te za pečat koji se kreira u ime pravne osobe.
- Kada se koristi XAdES podaci se upisuju kao xml komentar (samo tekst).

  Važno: *parametri se dostavljaju kako je gore navedeno i svi parametri su obavezni. Nije moguće izuzeće obaveznih parametara.*

  Datum i vrijeme potpisa/pečata

- Datum i vrijeme potpis/pečata na vizualu ne moraju nužno odgovarati datumu i vremenu samog kreiranja (i ugradnje) potpisa.
- Vizualni dio se priprema i ugrađuje prije samog potpisivanja, u tzv. presign procesu (metoda POST), kada se u dokument ugrađuje vizual i rezervira mjesto u dokumentu za ugradnju potpisne vrijednosti.
- Sam potpis se kreira u trenutku nakon što osoba unese PIN privatnog ključa a ugradnja potpisa se radi nakon potpisivanja, u tzv. postsign procesu (metoda PATCH), kada se u dokument ugrađuje sam potpis i opcionalno vremenski žig.
- Iz gore navedenog ukupnog procesa, u pravilu, datum i vrijeme potpisa/pečata na vizualu ne odgovaraju u potpunosti datumu i vremenu kreiranja potpisa (ili vremenskog žiga). Navedeno ponašanje je u skladu sa svim postojećim standardima i normama za kreiranje eIDAS kvalificiranog potpisa .
- Razlika u vremenu koje se nalazi na vizualu i vremenu koje je vidljivo prilikom validacije ovisi o vremenskom odmaku od pripreme podataka za potpis (presign proces) te samog kreiranja potpisa (sign proces) i ugradnje potpisa (i opcionalno kreiranja vremenskog žiga) u postsign procesu. Maksimalna razlika u vremenu odmaka određena je postavkama platforme. Postavka omogućava korisnicima da potpišu dokumente (aktiviraju potpisni ključ) u bilo kojem trenutku nakon što je dokument spreman za potpis, do isteka zadanog maksimalnog perioda.

5.3.4.2.1 Vrste vizuala

Podržani su sljedeći tipovi vizuala:

- Standardni vizual
  - uobičajenih dimenzija,
  - podržava standardni set podataka opisan u ovom dokumentu.
- Vizual manjih dimenzija od standradnog vizaula (‘small’)
  - visine 50% standardnog čime je omogućeno preciznije pozicioniranje elementa unutar stranice te veći broj elementa po stranici,
  - Koristi manji set podataka od uobičajenog.

Korištenje vizuala umanjenih dimenzija opisano je unutar odgovarajućih poglavlja ovog dokumenta te u prilozima.

5.3.5 WEB API parametri

5.3.5.1 PAdES parametri

5.3.5.1.1 Metoda POST za izračun HASH vrijednosti

Opis ulaznih parametara (upit)

	Parametar	Element	Tip	Obavezno	Primjer
1	token	-	string	DA	vrijednost dohvaćena od ePotpis rješenja (vidi 5.2.1).
2	signatureFormat	-	string	DA	"signatureFormat": "pades"
3	signatureType	-	string	DA	Potpis : "signatureType": "sign" Pečat : "signatureType": "seal"
4	addVisualData	-	bool	NE	Ugradnja vizuala : "addVisualData": true

4.1	addVisualDataOptions			NE	"addVisualData": true,
					"addVisualDataOptions": {
					"layoutId": "small"
					}

4.1.1		layoutId	string	NE **Opcionalno** – za vizual manjih dimenzija, ako je addVisualData=true • layoutId=small	
5	personNaturalData			NE **DA**, za potpis u privatne i poslovne svrhe, ako je zadovoljeno: • addVisualData=true **i** • signatureType=sign	"personNaturalData": { "nameSurname": "TEST TEST", "PIN": "12345678911", "PINCountry": "HR"}
5.1		PIN	string	DA	
5.2		nameSurname	string	NE	

5.3		PINCountry	string	DA	
6	personLegalData		string	NE **DA**, za pečat, ako je zadovoljeno: • addVisualData=true **i** signatureType=seal **Opcionalno -** za potpis u poslovne svrhe, ako je zadovoljeno: • addVisualData=true **i** signatureType=sign	"personLegalData": { "name": "Certilia d.o.o.", "VAT": "123465", "VATCountry": "HR", „sealName“ : „Odjel financija“ }
6.1		VAT	string		
6.2		name	string	NE	
6.3		sealName	string	NE	
7	addBlankPageOptions		string	NE **Opcionalno** - ako je zadovoljeno: • addVisualData=true	Dodaje praznu stranicu veličine i orijentacije zadnje stranice u dokumentu. " addBlankPageOptions „: { „blankPageOption“: „ADD_AUTO_ON_NO_SIGNATURES“}
7.1		blankPageOption	string	ADD_AUTO_ON_NO_SIGNATURES	
8	documents		niz	DA	"documents": [{ "verificationCode": "1feb229c-df…. ", "base64Document": base64Document....", "documentName": "Odluka o …", "firstRowMessage": "poruka usluge r1", "secondRowMessage": "poruka usluge r2", "thirdRowMessage": "poruka usluge r3", "pageNumber": 1, "pageLocation": 5}, { "verificationCode": "2aef349d-a1…. ", "base64Document": base64Document....", "documentName": "Zapisnik o …", "firstRowMessage": "poruka usluge r1", "secondRowMessage": "poruka usluge r2", "thirdRowMessage": "poruka usluge r3", "pageNumber": 2, "pageLocation": 12}…]

8.1		verificationCode	string	DA	vrijednost dohvaćena od ePotpis rješenja rješenja (vidi 5.2.1).
8.2		base64document	string, Base64	DA	base64 reprezentacija dokumenta koji se potpisuje.
8.3		documentName	string	NE	proizvoljan naziv dokumenta koji će se prikazivati umjesto generičkog naziva u ostalim komponentama sustava (npr. u mobilnoj aplikaciji).
8.4		firstRowMessage	string, max 60	NE	Proizvoljna poruka usluge redak 1 od 3
8.5		secondRowMessage	string, max 60	NE	Proizvoljna poruka usluge redak 2 od 3
8.6		thirdRowMessage	string, max 60	NE	Proizvoljna poruka usluge redak 3 od 3
8.7		pageNumber	int	NE **Opcionalno**, ako je addVisualData=true	Broj stranice na koji će se ugraditi vizual (ako postoji). Default = 0 - zadnja stranica. U default načinu rada (kad nije izričito specificiran broj stranice) ukoliko je stranica ispunjena potpisima na svim lokacijama ugradnja će se pokušati na prethodnoj stranici. Ukoliko nema slobodnh lokacija na stranicama dokumenta dolazi do greške i prekida se proces izračuna hash vrijednosti.
8.8		pageLocation	Int (0-12)	NE **Opcionalno**, ako je addVisualData=true	Broj lokacije (prema prilogu A) unutar stranice na koju će se ugraditi vizual. Default = 0 - prva slobodna lokacija. Ukoliko je spcificirana lokacija 1-12 a ista nije slobodna dolazi do greške i prekida se proces izračuna hash vrijednosti.

Tablica 5PAdESPOSTI: Ulazni parametri metoda POST

Opis izlaznih parametara (odgovor)

	Parametar	Element	Tip	Obavezno	Primjer
1	token	-	string	DA	vrijednost iz POST upita.
2	documents		niz	DA	"documents": [{"hash": "00ddc889a…95905df6b456c", "verificationCode": "65230190-29…"}, {"hash": "bedc5c506…326045fd36077", "verificationCode": "1adcd2a2-ea…"}, {"hash":"20be55be2…a7df4389b68c8", "verificationCode": "4ac4be81-c8e3-45…"}…]
2.1		verificationCode	string	DA	vrijednost iz POST upita.
		hash	string, hex	DA	hex reprezentacija hash vrijednosti koja se šalje na potpisivanje u koraku Zaprimanje hash-a (5.2.2).
		documentName	string	NE **DA**, ako je specificiran u POST pozivu.	proizvoljan naziv dokumenta iz POST upita.

Tablica 5PAdESPOSTO: Izlazni parametri metoda POST

5.3.5.1.2 Metoda PATCH za ugradnju potpisa

Opis ulaznih parametara (upit)

	Parametar	Element	Tip	Obavezno	Primjer
1	token	-	string	DA	vrijednost iz POST upita.
2	signatureFormat	-	string	DA	"signatureFormat": "pades"
3	signatureLevel	-	string	DA	Razina potpisa prema opisanim razinama u poglavlju (5.3). Nivo B_B : " signatureLevel ": "b" Nivo B_T : " signatureLevel ": "t" Nivo B_LT : " signatureLevel ": "lt" Nivo B_LTA : " signatureLevel ": "lta"
4	userCertificate	-	string, hex	DA	Hex reprezentacija X509 vrijednosti certifikata povezanog sa potpisanom hash vrijednošću iz odgovora poziva Vraćanje potpisanih podataka (5.2.4).
5	tsaAccess			NE **DA**, za nivo B_T, B_LT i B_LTA	Vrijednosti parametara kako je opisano u poglavlju 5.3. "tsaAccess": {"url": "https://tsa.certilia.com/qts", "username": "username", "password": "pass"}
5.1		url	string	DA	
5.2		username	string	DA	
5.3		password	string	DA	
6	documents		niz	DA	
6.1		verificationCode	string	DA	vrijednost iz POST upita.
6.2		hash	string, hex	DA	vrijednost iz POST odgovora.

6.3		signedHash	string, hex	DA	potpisna vrijednost iz procesa potpisivanja, odgovor poziva Vraćanje potpisanih podataka (5.2.4).

Tablica 5PAdESPATCHI: Ulazni parametri metoda PATCH

Opis izlaznih parametara (odgovor)

	Parametar	Element	Tip	Obavezno	Primjer
1	token	-	string	DA	vrijednost iz PATCH upita.
2	documents		niz	DA	"documents": [{"hash": "00ddc889a…95905df6b456c", "verificationCode": "65230190-29…"}, {"hash": "bedc5c506…326045fd36077", "verificationCode": "1adcd2a2-ea…"}, {"hash":"20be55be2…a7df4389b68c8", "verificationCode": "4ac4be81-c8e3-45…"}…]
2.1		verificationCode	string	DA	vrijednost iz PATCH upita.
		base64Document	string, base64	DA	Base64 reprezentacija dokumenta sa ugrađenim poptisom.

Tablica 5PAdESPATCHO: Izlazni parametri metoda PATCH

5.3.5.2 XAdES parametri

5.3.5.2.1 Metoda POST za izračun HASH vrijednosti

Opis parametara (upit)

	Parametar	Element	Tip	Obavezno	Primjer
1	token	-	string	DA	vrijednost dohvaćena od ePotpis rješenja (vidi 5.2.1).
2	signatureFormat	-	string	DA	"signatureFormat": "xades"
3	signatureType	-	string	DA	Potpis : "signatureType": "sign" Pečat : "signatureType": "seal"
4	addVisualData	-	bool	NE	Ugradnja xml komentara : "addVisualData": true
5	personNaturalData			NE **DA**, za potpis u privatne i poslovne svrhe, ako je zadovoljeno: • addVisualData=true **i** • signatureType=sign	"personNaturalData": { "nameSurname": "TEST TEST", "PIN": "12345678911", "PINCountry": "HR"}
5.1		PIN	string	DA	
5.2		nameSurname	string	NE	
5.3		PINCountry	string	DA	
6	personLegalData		string	NE **DA**, za pečat, ako je zadovoljeno: • addVisualData=true **i** signatureType=seal	"personLegalData": { "name": "Certilia d.o.o.", "VAT": "123465", "VATCountry": "HR",

				Opcionalno - za potpis u poslovne svrhe, ako je zadovoljeno: • addVisualData=true **i** signatureType=sign	„sealName“ : „Odjel financija“ },
6.1		VAT	string		
6.2		name	string	NE	
6.3		sealName	string	NE	
7	documents		niz	DA	"documents": [{ "verificationCode": "1feb229c-df…. ", "base64Document": base64Document....", "firstRowMessage": "poruka usluge r1", "secondRowMessage": "poruka usluge r2", "thirdRowMessage": "poruka usluge r3"}, { "verificationCode": "2aef349d-a1…. ", "base64Document": base64Document....", "firstRowMessage": "poruka usluge r1", "secondRowMessage": "poruka usluge r2", "thirdRowMessage": "poruka usluge r3"},…]
7.1		verificationCode	string	DA	vrijednost dohvaćena od ePotpis rješenja (vidi 5.2.1).
7.2		base64document	string	DA	Base64 reprezentacija dokumenta koji se potpisuje.
7.3		firstRowMessage	string, max 60	NE	Proizvoljna poruka usluge redak 1 od 3
7.4		secondRowMessage	string, max 60	NE	Proizvoljna poruka usluge redak 2 od 3
7.5		thirdRowMessage	string, max 60	NE	Proizvoljna poruka usluge redak 3 od 3

Tablica 5XAdESPOSTI: Ulazni parametri metoda POST

Opis izlaznih parametara (odgovor)

	Parametar	Element	Tip	Obavezno	Primjer
1	token	-	string	DA	vrijednost iz POST poziva.
2	documents		niz	DA	"documents": [{"hash": "00ddc889a…95905df6b456c", "verificationCode": "65230190-29…"}, {"hash": "bedc5c506…326045fd36077", "verificationCode": "1adcd2a2-ea…"}, {"hash":"20be55be2…a7df4389b68c8", "verificationCode": "4ac4be81-c8e3-45…"}…]
2.1		verificationCode	string	DA	vrijednost iz POST upita.
		hash	string, hex	DA	hex reprezentacija hash vrijednosti koja se šalje na potpisivanje.

Tablica 5XAdESPOSTO: Izazni parametri metoda POST

5.3.5.2.2 Metoda PATCH za ugradnju potpisa

Opis ulaznih parametara (upit)

	Parametar	Element	Tip	Obavezno	Primjer
1	token	-	string	DA	vrijednost iz POST upita.
2	signatureFormat	-	string	DA	"signatureFormat": "xades"
3	signatureLevel	-	string	DA	Nivo B_B : " signatureLevel ": "b" Nivo B_T : " signatureLevel ": "t" Nivo B_LT : " signatureLevel ": "lt" Nivo B_LTA : " signatureLevel ": "lta"
4	userCertificate	-	string, hex	DA	Hex reprezentacija X509 vrijednosti certifikata povezanog sa potpisanom hash vrijednošću iz odgovora poziva Vraćanje potpisanih podataka (5.2.4).
5	tsaAccess			NE **DA**, za nivo B_T, B_LT i B_LTA	Vrijednosti parametara kako je opisano u poglavlju 5.3. "tsaAccess": {"url": "https://tsa.certilia.com/qts", "username": "username", "password": "pass"}
5.1		url	string	DA	
5.2		username	string	DA	
5.3		password	string	DA	
6	documents		niz	DA	
6.1		verificationCode	string	DA	vrijednost iz POST upita.
6.2		hash	string, hex	DA	vrijednost iz POST odgovora.

6.3		signedHash	string, hex	DA	potpisna vrijednost iz procesa potpisivanja, odgovor poziva Vraćanje potpisanih podataka (5.2.4).

Tablica 5XAdESPATCHI: Ulazni parametri metoda PATCH

Opis izlaznih parametara (odgovor)

	Parametar	Element	Tip	Obavezno	Primjer
1	token	-	string	DA	vrijednost iz PATCH poziva.
2	documents		niz	DA	"documents": [{"hash": "00ddc889a…95905df6b456c", "verificationCode": "65230190-29…"}, {"hash": "bedc5c506…326045fd36077", "verificationCode": "1adcd2a2-ea…"}, {"hash":"20be55be2…a7df4389b68c8", "verificationCode": "4ac4be81-c8e3-45…"}…]
2.1		verificationCode	string	DA	vrijednost iz PATCH upita.
		base64Document	string, base64	DA	Base64 reprezentacija dokumenta sa ugrađenim poptisom.

Tablica 5XAdESPATCHO: Izazni parametri metoda PATCH

5.3.5.3 PAdES Web API primjeri

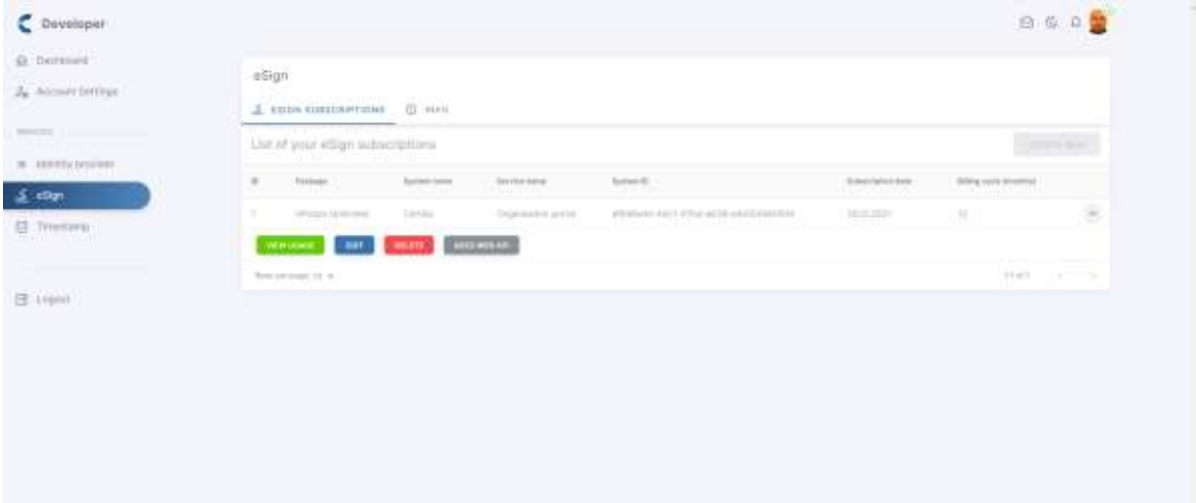
5.3.5.3.1 Računanje hash vrijednosti PDF dokumenta (PreSign)

Protokol: HTTPS

URL:
[PROD]: https://api.certilia.com/pades/v2
[TEST] : https://api.test.certilia.com/pades/v2

HTTP Metoda: POST

Sigurnost: SSL(TLS1.2, TLS1.3)
Header: Authorization: Bearer TOKEN_VALUE
Napomena: TOKEN_VALUE je potrebno generirati putem Certilia Developer portala (https://developer.certilia.com), klikom na opciju ADES WEB API



5.3.5.3.2 Upit

```
JSON DATA:
{
	"token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0cmFjZUlkIjoiYzJjZDZlZTMtOTc0ZS00N2FmLTg0NmMtMGNhZWJjYmNiYjJlIiwiaWF0IjoxNjAwNzY1NTQ5LCJleHAiOjE2MDA3NjczNDl9.gWux0wgg9a1rvviK2x8Fcc9hqLW0nUkW7Ty14svuH4s",
	"signatureFormat": "pades",
	"signatureType": "sign",
	"addVisualData": true,
	"personNaturalData": {
		"nameSurname": "IVO IVIĆ",
		"PIN": "x",
		"PINCountry": "HR"
	},
	"personLegalData": {
		"name": "AKD",
```

```
                "VAT": "58843087891",
                "VATCountry": "HR",
                "sealName" : "pecat"
        },
        "documents": [
                {
                        "verificationCode": "1feb229c-b0b5-4417-9cbc-555c270c7733",
                        "base64Document": "base64Document....",
                        "documentName": "Odluka o provedbi popisa uredskog materijala.pdf",
                        "firstRowMessage": "Custom poruka usluge redak #1#1",
                        "secondRowMessage": "Custom poruka usluge redak #1#2",
                        "thirdRowMessage": "Custom poruka usluge redak #1#3",
                        "pageNumber": 1,
                        "pageLocation": 5
                }
        ]
}
```


5.3.5.3.3 Odgovor


```
JSON DATA:
{
        "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0cmFjZUlkIjoiYzJjZDZlZTMtOTc0ZS00N2FmLTg0NmMtMGNhZW
JjYmNiYjJlIiwiaWF0IjoxNjAwNzY1NTQ5LCJleHAiOjE2MDA3NjczNDl9.gWux0wgg9a1rvviK2x8Fcc9hqLW0nUk
W7Ty14svuH4s",
        "documents": [
                {
                        "hash":
"65D2CB105AB0A3EE2EE9DD6FF2E8A4AD40E8AA34E1FEE5A9F0A0EC3D762C979B",
                        "verificationCode": "1feb229c-b0b5-4417-9cbc-555c270c7733",
                        "documentName": "Naziv dokumenta1.ext"  //ako je definiran kod poziva
                },
                {
                        "hash":
"D21868BFE588F6F167B9AFDDA5DDC0A9291C707C0CC675591200AC3EE018BFB2",
                        "verificationCode": "854dbc5a-a19f-44f3-988f-972e5b45c46f",
                        "documentName": "Naziv dokumenta2.ext"  //ako je definiran kod poziva
                },
                {
                        "hash":
"A63257EBD3FF9A72A38F70A7584A4B5E64FF74CF7E34703A9AC7511FE2BA2D3A",
                        "verificationCode": "941adf50-6007-4b16-803f-db4bf3eff8bc",
                        "documentName": "Naziv dokumenta3.ext"  //ako je definiran kod poziva
                }
        ]
}
```

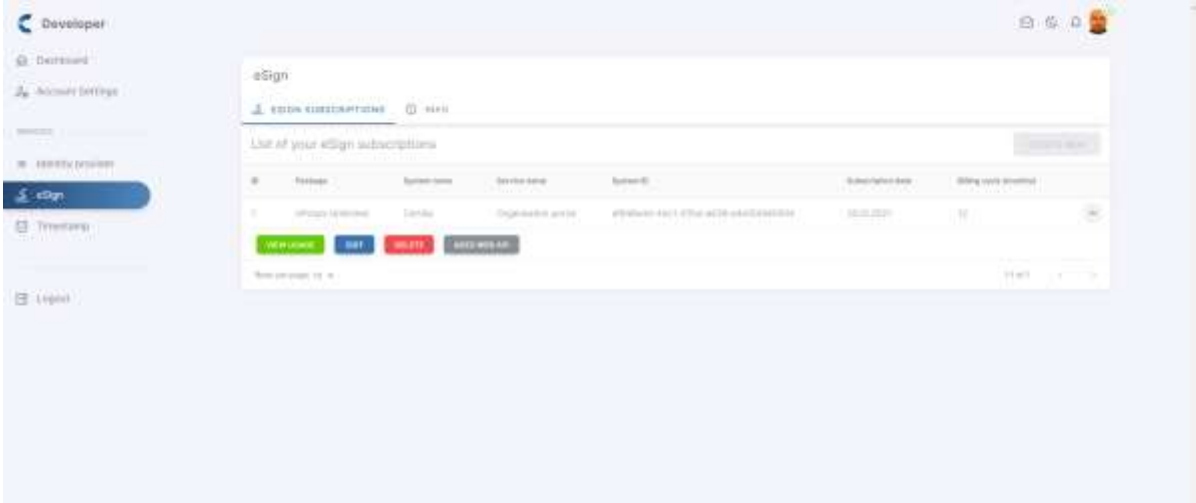

5.3.5.3.4 Ugradnja potpisane vrijednosti u PDF dokument (PostSign)

Protokol: HTTPS

URL:
[PROD]: https://api.certilia.com/pades/v2
[TEST] : https://api.test.certilia.com/pades/v2

HTTP Metoda: PATCH

Sigurnost: SSL(TLS1.2, TLS1.3)
Header: Authorization: Bearer TOKEN_VALUE
Napomena: TOKEN_VALUE je potrebno generirati putem Certilia Developer portala (https://developer.certilia.com), klikom na opciju ADES WEB API



5.3.5.3.5 Upit

```
JSON DATA:
{
	"token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0cmFjZUlkIjoiODJlZGY2MGItZWJjNS00MWY5LTkzNTAtODg0NzU
yNWE1YTg2IiwiaWF0IjoxNjAwNzY1ODg0LCJleHAiOjE2MDA3Njc2ODR9.jV9LxpcBiol0emhSZpli9qpw_PSLw9
Z5qyyogsFlTgo",
	"signatureFormat": "pades",
	"signatureLevel": "t",
	"userCertificate": "308206663082044EA00302010202085D5CA8…",
	"tsaAccess": {
		"url": "https://tsa.certilia.com/qts",
		"username": "x",
		"password": "x"
	},
	"documents": [
		{
			"verificationCode": "97c9dc10-d34e-414f-a9e6-27c25b0fd321",
			"hash":
"F4BC0B0C7876E55FCA96A52B5EDCC92473F2592F8C9DA04C0DA33FD4AEE9652A",
			"signedHash":
"6CA003ED5CC8F4E57A2B9EF8B18D640A5A2B69FAC5F38D048BD8D758BF7D84F80726D74C9C784A1A46
```

```
5A9733F0EF9E21BD030B56F820AB1AE210C3A84C58E49660D51A2452EE14AF6A64D9A0FD47A59C211CB
2983BBBF6142CA5930D96A3962C3779016DEB349ACCFCC872B83658EAAB8EDDE28CC8DF529219E1CC47
B4DDC796B13318E2B5D608DE587D35047402867A03A9B9730A8D6B3F51063A2EA8D43DE6A8162F29320
F9B0120A88ABD963831E90E77D2E6D9C7742CAD9067571ED0648B8141EB6EE4D946764E933C75959217
DA34B5D5FCB23611CD7B71A75397F1EDF6ED55E3EC9D6969CF6756C8F86B4202155FC7EE8773C3AA6424
412C01CE6AD1A4"
                }
        ]
}
```

5.3.5.3.6 Odgovor

```
JSON DATA:
{
        "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0cmFjZUlkIjoiODJlZGY2MGItZWJjNS00MWY5LTkzNTAtODg0NzU
yNWE1YTg2IiwiaWF0IjoxNjAwNzY1ODg0LCJleHAiOjE2MDA3Njc2ODR9.jV9LxpcBiol0emhSZpli9qpw_PSLw9
Z5qyyogsFlTgo",
        "documents": [
                {
                        "verificationCode": "97c9dc10-d34e-414f-a9e6-27c25b0fd321",
                        "base64Document": " base64Document...",
                        "documentName": "Naziv dokumenta.ext"  //ako je definiran kod POST poziva
                }
        ]
}
```

5.3.5.4 XAdES Web API primjeri

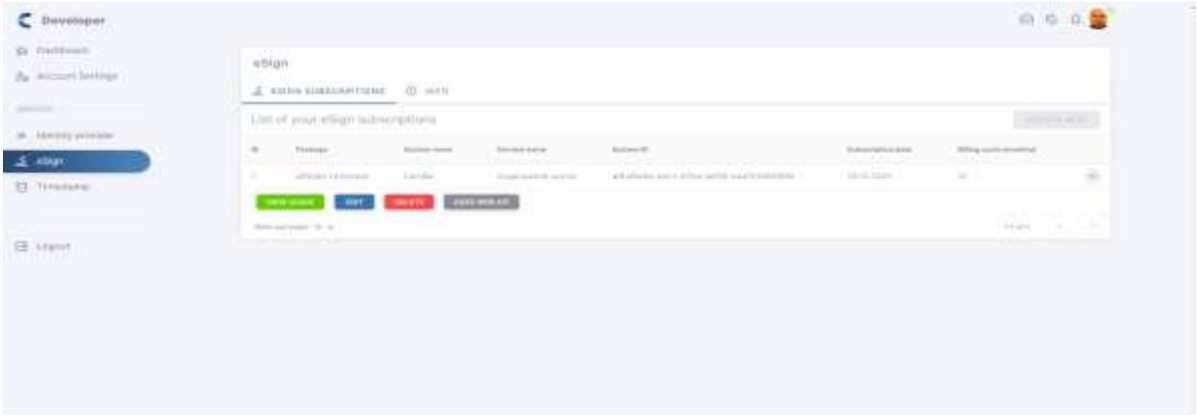
5.3.5.4.1 Računanje hash vrijednosti XML dokumenta (PreSign)

Protokol: HTTPS

URL:
[PROD]: https://api.certilia.com/xades/v1
[TEST] : https://api.test.certilia.com/xades/v1

HTTP Metoda: POST

Sigurnost: SSL(TLS1.2, TLS1.3)
Header: Authorization: Bearer TOKEN_VALUE
Napomena: TOKEN_VALUE je potrebno generirati putem Certilia Developer portala (https://developer.certilia.com), klikom na opciju ADES WEB API



5.3.5.4.2 Upit

```
JSON DATA:
{
        "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0cmFjZUlkIjoiZjAxNGY3NjMtYmY5MS00MWI1LWE3MzUtNzRiOTMzYTIyMTRiIiwiaWF0IjoxNjM4Nzg4OTQ2LCJleHAiOjE2Mzg4MTc3NDZ9.osmG_0mg6XjYuZxAujTFGlt3RGflpTpwzDrXZtY7U8A",
        "signatureFormat": "xades",
        "signatureType": "sign",
        "addVisualData": false,
        "documents": [
                {
                        "verificationCode": "f3df6aca-1927-46b5-8267-e24849d5c340",
                        "base64Document": " base64Document…"
                }
        ]
}
```

5.3.5.4.3 Odgovor

JSON DATA:
{
"token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0cmFjZUlkIjoiZjAxNGY3NjMtYmY5MS00MWI1LWE3MzUtNzRiOTMzYTIyMTRiIiwiaWF0IjoxNjM4Nzg4OTQ2LCJleHAiOjE2Mzg4MTc3NDZ9.osmG_0mg6XjYuZxAujTFGlt3RGflpTpwzDrXZtY7U8A",
"documents": [
{
"hash":
"CE895C3D750C088ADE7F42274B42A1829612EAEEC9E9282B004A63FFF3230A55",
"verificationCode": "f3df6aca-1927-46b5-8267-e24849d5c340"
}
]
}

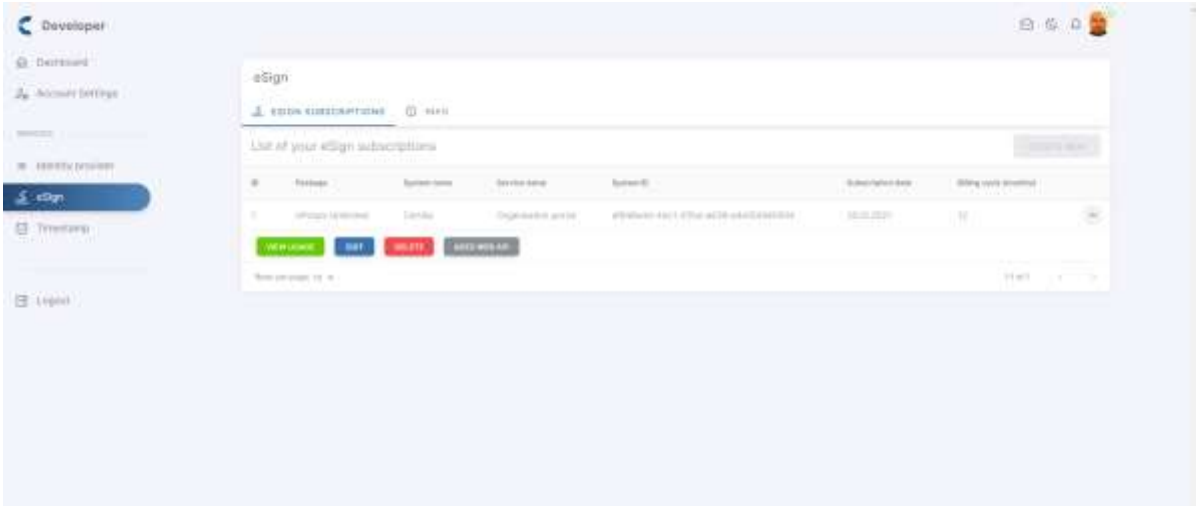
5.3.5.4.4 Ugradnja potpisane vrijednosti u XML dokument (PostSign)

Protokol: HTTPS

URL:
[PROD]: https://api.certilia.com/xades/v1
[TEST] : https://api.test.certilia.com/xades/v1

HTTP Metoda: PATCH

Sigurnost: SSL(TLS1.2, TLS1.3)
Header: Authorization: Bearer TOKEN_VALUE
Napomena: TOKEN_VALUE je potrebno generirati putem Certilia Developer portala (https://developer.certilia.com), klikom na opciju ADES WEB API



5.3.5.4.5 Upit

JSON DATA:

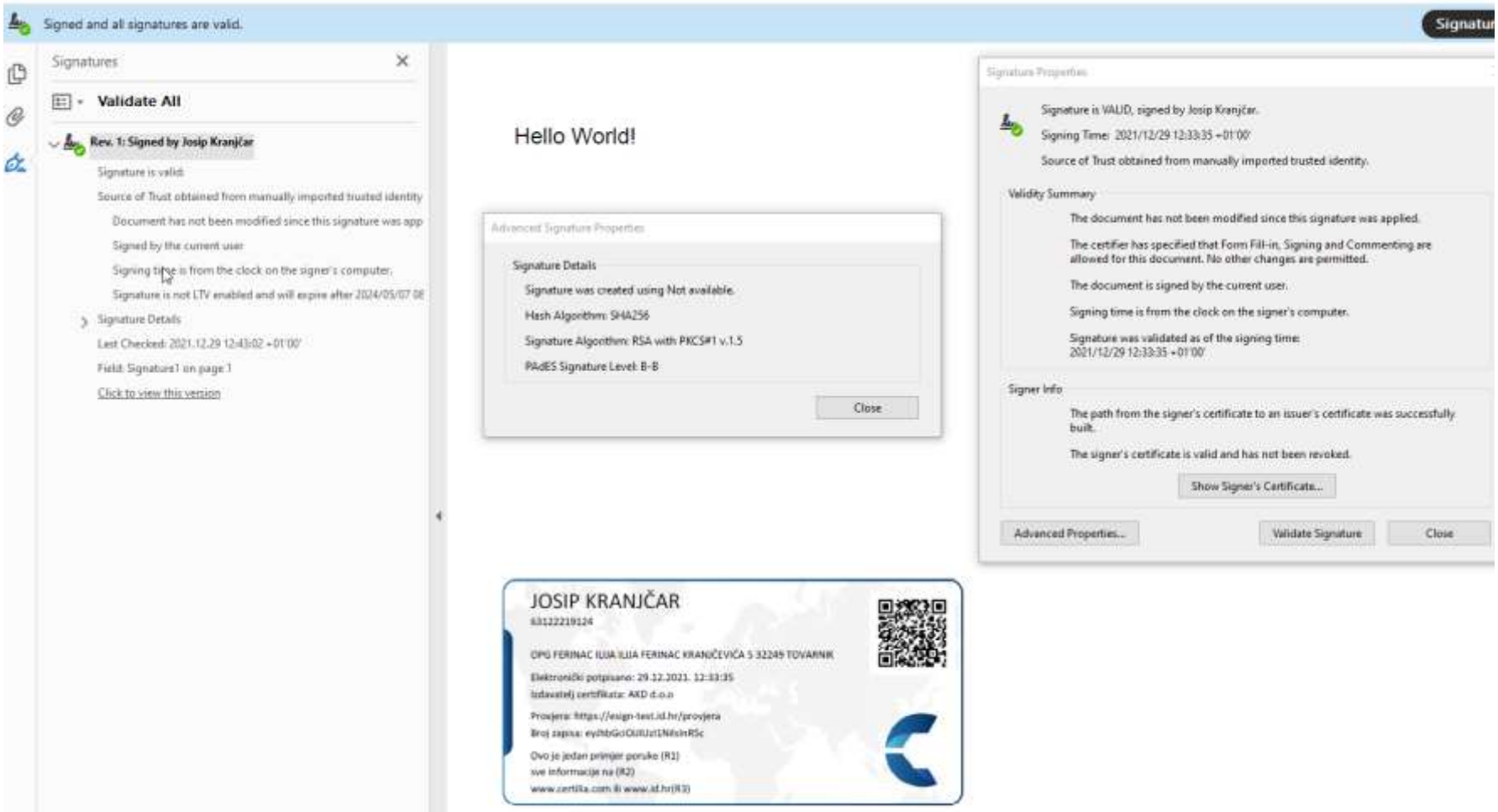

```
{
	"token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0cmFjZUlkIjoiZjAxNGY3NjMtYmY5MS00MWI1LWE3MzUtNzRiO
TMzYTIyMTRiIiwiaWF0IjoxNjM4Nzg4OTQ2LCJleHAiOjE2Mzg4MTc3NDZ9.osmG_0mg6XjYuZxAujTFGlt3RGfl
pTpwzDrXZtY7U8A",
	"signatureFormat": "xades",
	"signatureLevel": "lta",
	"userCertificate":
"308206D6308204BEA003020102021100BAA88373CC6EB858000000005F24190F300D06092A864886F70
D01010B05003048310B30090603550406130248523 11D301B060355040A131446696E616E63696A736B6
1206167656E63696A61311A3018060355040313114669 6E612044656D6F204341203230323030 1E170D32
303131313132303132343 05A170D32353131313132303132343 05A30819D310B30090603550406130248 5
2311230100603550 40A1309544553542044 2E442E3116301406035504611 30D485231313131393939
3938310F300D060355040713065A4147524542310F300D060355040413065445535445 49310D300B06035
5042A13045445535431143012060355040313 0B5445535420544553544E49311B3019060355040513124 8
523131313131303030303037 2E312E333030820122300D06092A864886F70D0101010500038201 0F00308
2010A0282010100C103ECCB28A6860BE2413D80294066170805EF36664A200E7CCB2A98BDCC929199706
83A0B11D88B411560057B22DDCEDA823971957E52D0F3D98F8758D38C57BBCEEA111E91B5AFBF3ECA61
871059A8D92B092A7057FC7C4E3F1CA3D7E80FC6A1BF8911995FB54E3C379FC830CE76229295B5B88063
6A6E49178176DC419ED33062319E3FFDB4F9B7EAC88027EBF22B90F78DBE20397D64635CAF1EC6D02D06
8F7D6C101556B6BBF52574C052760B43CA1EC6F809164BE5515EBE3045BA6797D28EC8040E6EABF96C78
CE32CCAA0ADC85A096E2B74B2D226CBBD4C038015E457CC20813F9E651803E7ED0FDA2F21756070F1E16
316C00D07DEEFFE2A1D9C4090203010001A3820263308202 5F300E0603551D0F0101FF0404030205A0301
D0603551D250416301406082B0601050507030406082B0601050507030 23081AC0603551D200481A4308
1A130819406092B7C885005210C0301308186304106082B0601050507020116356874747 03A2F2F64656D
6F2D706B692E66696E612E68722F6370732F6370736E716364656D6F3230313476322D302D68722E70646
6304106082B0601050507020116356874747 03A2F2F64656D6F2D706B692E66696E612E68722F6370732F
6370736E716364656D6F3230313476322D302D656E2E706466300806060400 8F7A0101307D06082B06010
5050701010471306F302806082B0601050507300 1861C687474703A2F2F64656D6F323031342D6F637370
2E66696E612E6872304306082B0601050507300 28637687474703A2F2F64656D6F2D706B692E66696E612
E68722F636572746966696B6174692F64656D6F323032305F7375625F63612E6365723081B40603551D1F
0481AC3081A93081A6A081A3A081A08628687474703A2F2F64656D6F2D706B692E66696E612E68722F63
726C2F64656D6F323032302E63726C86746C6461703A2F2F64656D6F2D6C6461702E66696E612E68722F6
36E3D46696E6125323044656D6F2532304341253230323032302C6F3D46696E616E63696A736B61253230
6167656E63696A612C633D48523F6365727469666963617465526576F636174696F6E4C6973742533426
2696E617279301F0603551D2304183016801495AF52D5C2E9D737843E6E498FC91FEA5C2B5FCF301D0603
551D0E04160414A4DAFE372C89C7AAAA298973E0D554622BD4586B30090603551D1304023000300D060
92A864886F70D01010B05000382020100 9FD70174BFC46B3EF8672C55EF92667CF7F98DB2B9170FE4A761
B73D0E06FF0CEC6A47D18538B40590A058EA7C4C2863095053E7E3D65902911CBF9403E2DE92E390A0C5
263BC666CB584170259F45031EDE49438D4B041604949D361A62E09F8DE632CD508A5CB0564DBD3C398
CC16428804A27F3A8B40DC47AC3FD4A0ADE1FEBB27FB6BDD710C19DBB4EC5492C0727FCAA6004BE287B
6D9784E539166976D53A72511369F04B818A5E8F10F42C43F21563665EC66AA9ACAE0E54A2C03FA7C6BD
4141D8AC67A86B763C46B0D9E0FCE89ADF7D1FFCA7BDAF70F31A35586D0019A7417ABF034A5DE328F46
3E3AD92C5439D91980983420F38350D2B0D3FDFF3FFFC80E9447F8B9FECCE848B34F3715E95142F331A9C
9685F8E2A0FBF924600A22B01E2A4AEA8FDC3DC5952E056B47CD16526E631773855AD6E9C9611D7AB97
484F9D3ACC14414F13918D751877A5F8909CE4BA6456513A82365546A7A461EC7109B5E69771A13C8275
3CDB2DBF9BE41F6502ED29A27750932C9117268E9B07EAA33494D03D73E0460A5D45A2157255F7B29D3
07F87DCB520A35EB5D008C8B42F8C8907981B14BEC93BDF5B774D99AF695A2CA0887DD054C97437C178
3506D13480207E73A954F0299605205D1532C27BDDDC8306AAF2B355982AA15037726F843883992AF1CF
6A6AE921EEB1F289896F9CF8978328D935D7EEA795899BFA5442E",
	"tsaAccess": {
		"url": "https://tsa.certilia.com/qts",
```

```
                "username": "x",
                "password": "x"
        },
        "documents": [
                {
                        "verificationCode": "f3df6aca-1927-46b5-8267-e24849d5c340",
                        "hash":
"CE895C3D750C088ADE7F42274B42A1829612EAEEC9E9282B004A63FFF3230A55",
                        "signedHash":
"3061B206C1AC585B3D4600099E3E0C646BDAFEDF34F3CB0AD4176ABB7E138CEAB1F1E670BD5FB4DC02
0E863745CBBF4FA59C6B3868092686219D2D6861585B8BA4902293FC35A09D112E23769C540327CED8A4
BEC8D24374EE1A0053F1ED94AF24CE47B95BA3570915721F8A1860C7DBF94AAB49AC33CCDDED9D4C505
D4BD04FE7FADC28FB615156AED01EFFCC0CB8C2A6F1078B5FA6562DA79BDDF5865A61BF67408E737863
32F941DA893980A042D4490AAF0226DD0ECB6DD048EC91B73334D3E5ADB659C8CE27348B5C4C3BA700F
8CB926D0DB566FF19F17807E27C770DA3DBF54C47A381AFB5130F033A7F4F0F2F3D23EDB222C5BF39808
6DDF935E18F80",
                        "timeStamp": "323032312D31322D30365431313A30393A31375A"
                }
        ]
}
```

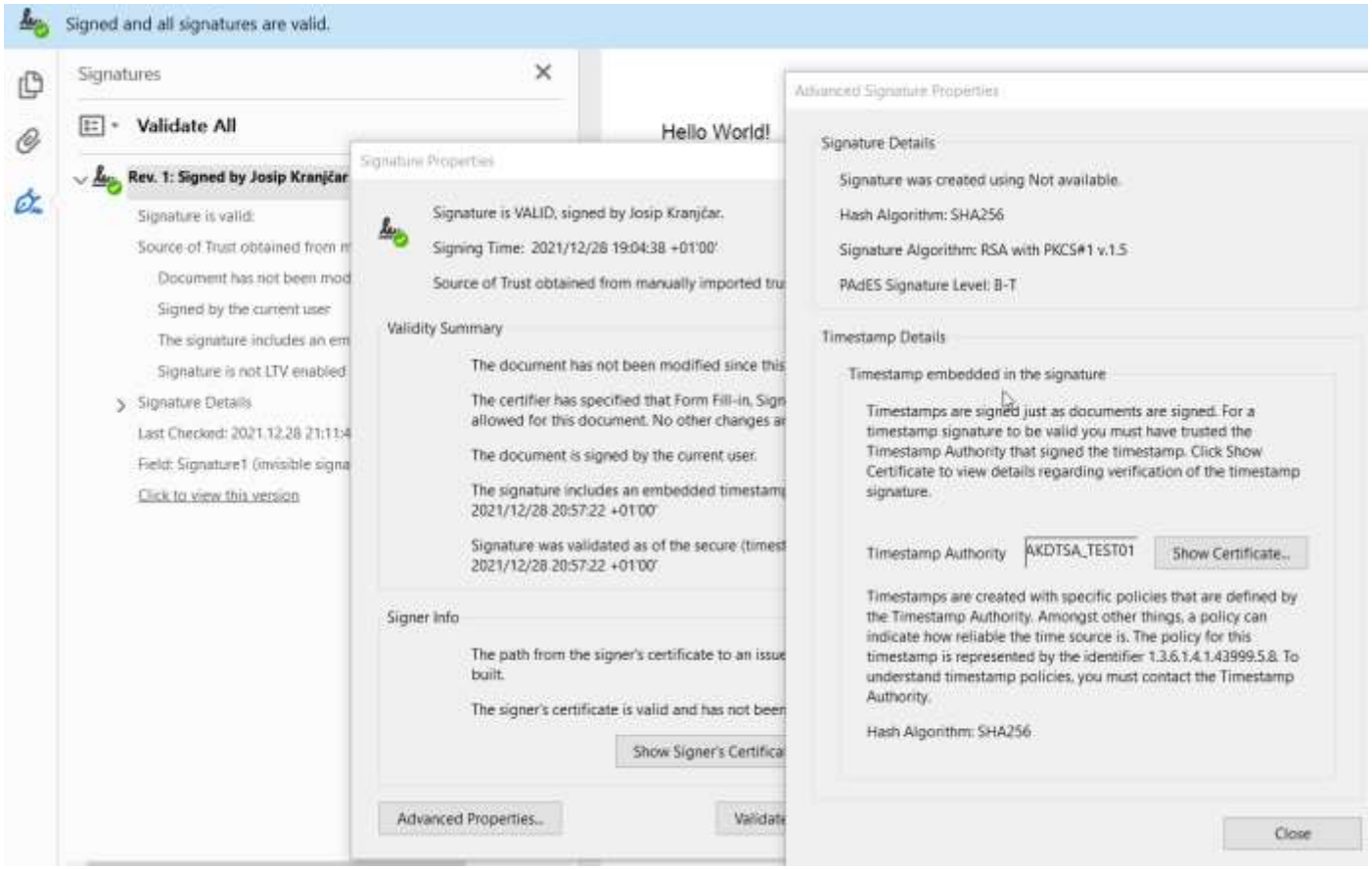

5.3.5.4.6 Odgovor


```
JSON DATA:
{
        "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0cmFjZUlkIjoiZjAxNGY3NjMtYmY5MS00MWI1LWE3MzUtNzRiO
TMzYTIyMTRiIiwiaWF0IjoxNjM4Nzg4OTQ2LCJleHAiOjE2Mzg4MTc3NDZ9.osmG_0mg6XjYuZxAujTFGlt3RGfl
pTpwzDrXZtY7U8A",
        "documents": [
                {
                        "verificationCode": "f3df6aca-1927-46b5-8267-e24849d5c340",
                        "base64Document": " base64Document… "
                }
        ]
}
```

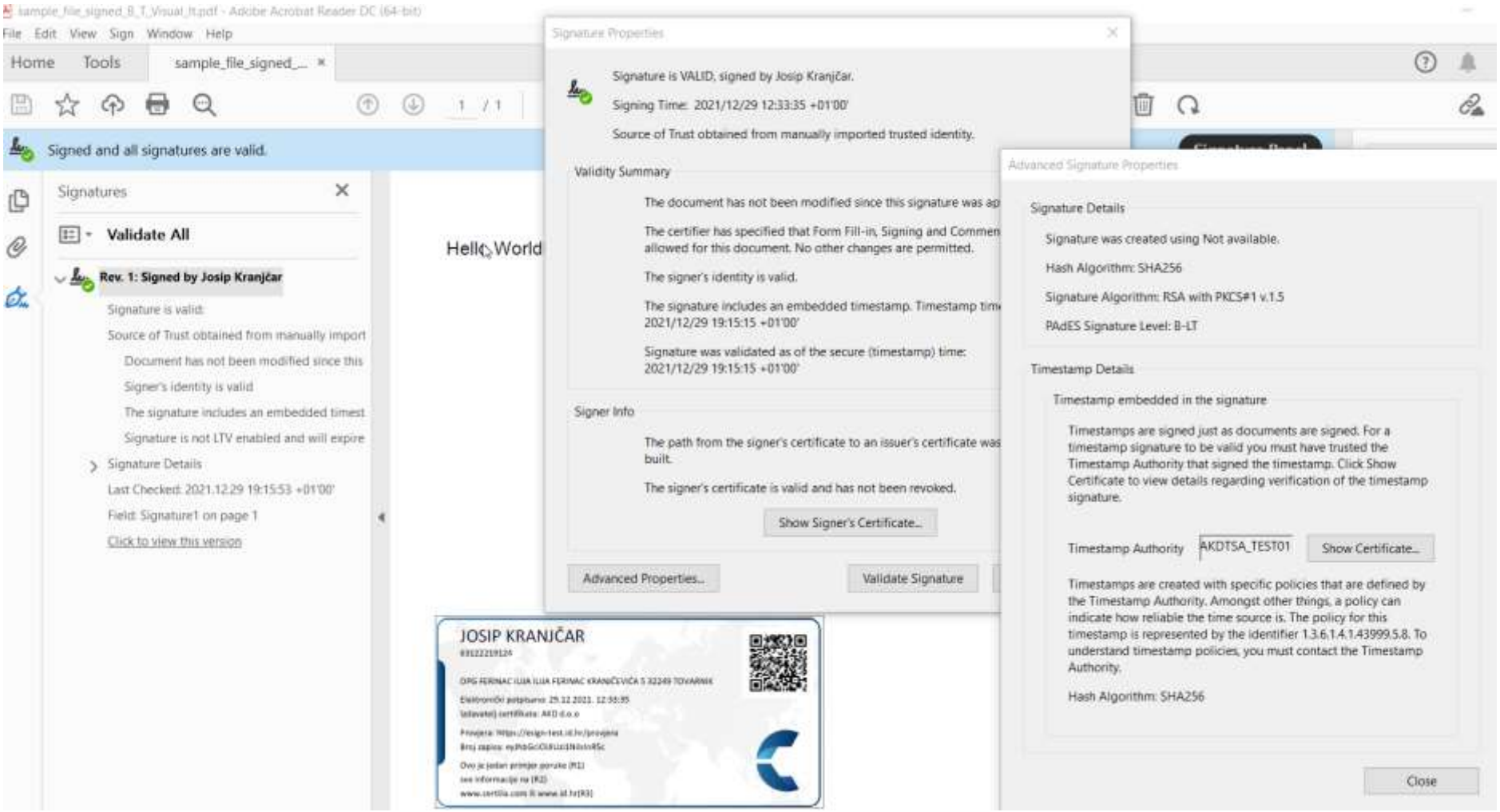
5.3.6 Provjera potpisa u Acrobat Readeru



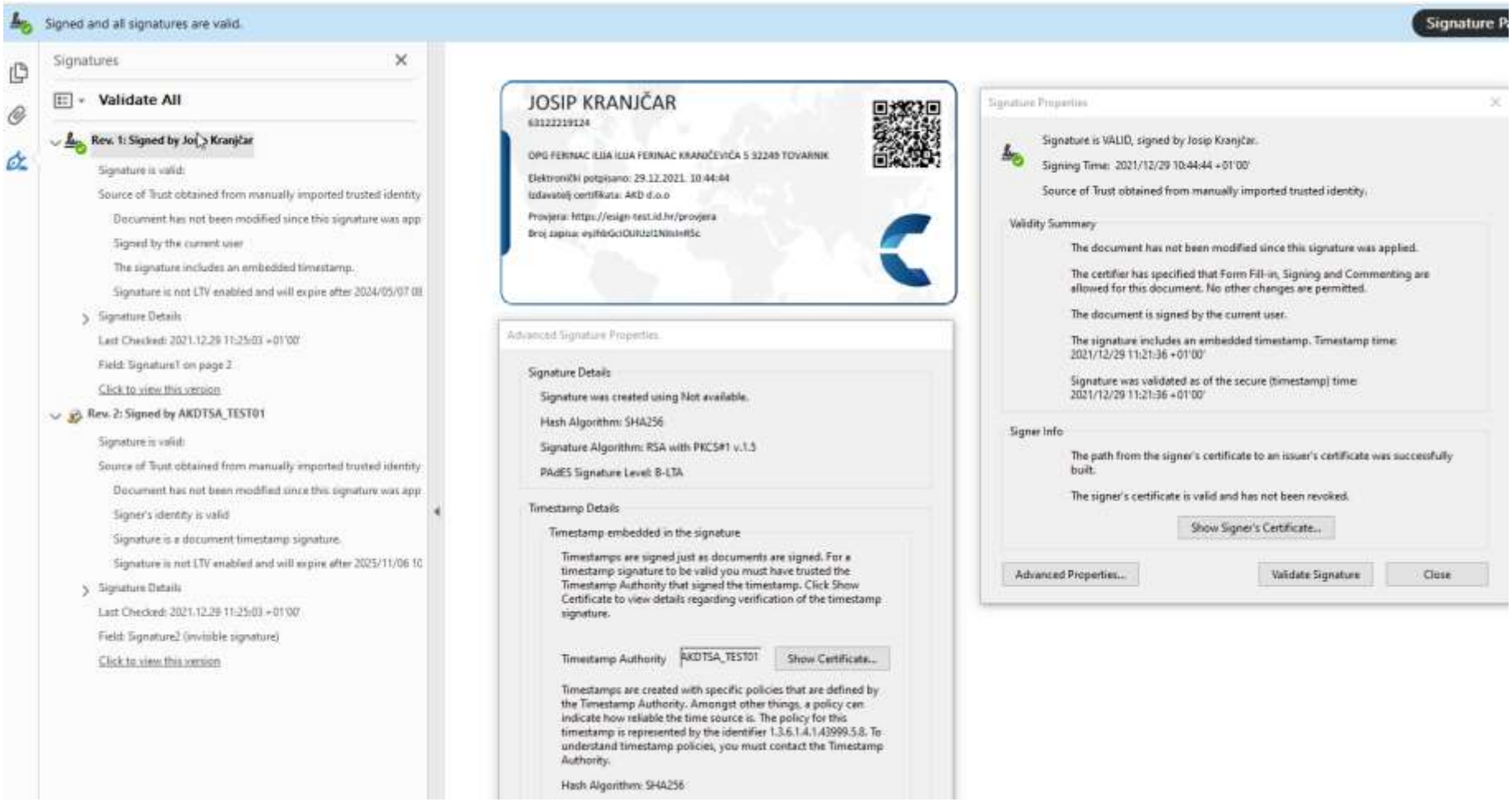
Slika B-B_Visual: Validacija u Adobe Readeru, pageNumber = 1, pageLocation = 5



Slika B-T_No_Visual: Validacija u Adobe Readeru



Slika B-LT_Visual: Validacija u Adobe Readeru, pageNumber = 1, pageLocation = 5



Slika B-LTA_Visual_No_Messages: Validacija u Adobe Readeru

5.3.7 Greške

Default lokalizacija za polje Description je uvijek **HR** te promjena na WEB API servisima nije moguća.

5.3.7.1 PAdES

Primjeri:


```
 "Version": "PAdES-AllInOne,15.03.2024. 12:47:32",
  "Note": "For PAdES/XAdES/nAdES.",
  "Platforms": "Certilia, MU_SDURD.",
  "SampleErrorMessages": [
   "{ Error = { Type = HG_INVALID_REQUEST, Code = 65, Message = INVALID_PERSON_NAME_SURNAME, Description = Neispravno ime i prezime osobe. } }",
   "{ Error = { Type = HG_INVALID_REQUEST, Code = 65, Message = INVALID_PERSON_NAME_SURNAME, Description = Invalid person's name and surname. } }",
   "{ Error = { Type = HPDF_DOCUMENT_SECURITY_ERROR, Code = 6203, Message = PDF_PASSWORD_PROTECTED, Description = Pdf dokument je zaštićen zaporkom. } }",
   "{ Error = { Type = HPDF_DOCUMENT_SECURITY_ERROR, Code = 6203, Message = PDF_PASSWORD_PROTECTED, Description = Pdf document is password protected. } }",
   "{ Error = { Type = HPDF_DOCUMENT_SECURITY_ERROR, Code = 6204, Message = PDF_IS_ENCRYPTED, Description = Pdf dokument je kriptiran. } }",
   "{ Error = { Type = HG_INVALID_REQUEST, Code = 66, Message = INVALID_PERSON_PIN, Description = Neispravan OIB osobe. } }",
   "{ Error = { Type = HS_INVALID_SIGNATURE_DATA_VISUAL, Code = 687, Message = SIGNATURE_VISUAL_LOCATION_ON_PAGE_NOT_AVAILABLE, Description = Lokacija na stranici nije
dostupna za ugradnju vizuala. } }",
   "{ Error = { Type = HG_INVALID_REQUEST, Code = 650, Message = UNSUPPORTED_SIGNATURE_LEVEL, Description = Invalid eIDAS signature level. } }",
   "{ Error = { Type = HG_INVALID_REQUEST, Code = 680, Message = INVALID_SIGNATURE_VALUE, Description = Invalid signature value. } }",
   "{ Error = { Type = HG_INVALID_REQUEST, Code = 616, Message = INVALID_VERIFICATION_CODE, Description = Invalid verification code. } }",
   "{ Error = { Type = HG_INVALID_REQUEST, Code = 660, Message = INVALID_TSA_URL, Description = Neispravan URL TSA servisa. } }",
   "{ Error = { Type = HL_INVALID_AUTHORIZATION_CREDENTIALS, Code = 664, Message = INVALID_TSA_CREDENTIALS, Description = Neispravni autorizacijski podaci. } }",
   "{ Error = { Type = HS_INVALID_SIGNATURE_DATA, Code = 681, Message = SIGNATURE_NOT_VERIFIED, Description = Neuspješna verifikacija potpisa. } }",
   "{ Error = { Type = HUC_INVALID_USER_CERTIFICATE, Code = 677, Message = USER_CERTIFICATE_EXPIRED, Description = Korisnički certifikat je istekao. } }",
   "{ Error = { Type = HG_INVALID_REQUEST, Code = 610, Message = INVALID_ORGANIZATION_NAME, Description = Invalid organzation's name. } }",
   "{ Error = { Type = HG_INVALID_REQUEST, Code = 611, Message = INVALID_ORGANIZATION_VAT, Description = Invalid organzation's VAT. } }",
   "{ Error = { Type = HG_INVALID_REQUEST, Code = 610, Message = INVALID_ORGANIZATION_NAME, Description = Neispravan naziv organizacije. } }",
   "{ Error = { Type = HG_INVALID_REQUEST, Code = 611, Message = INVALID_ORGANIZATION_VAT, Description = Neispravan OIB organizacije. } }"
  ]
```

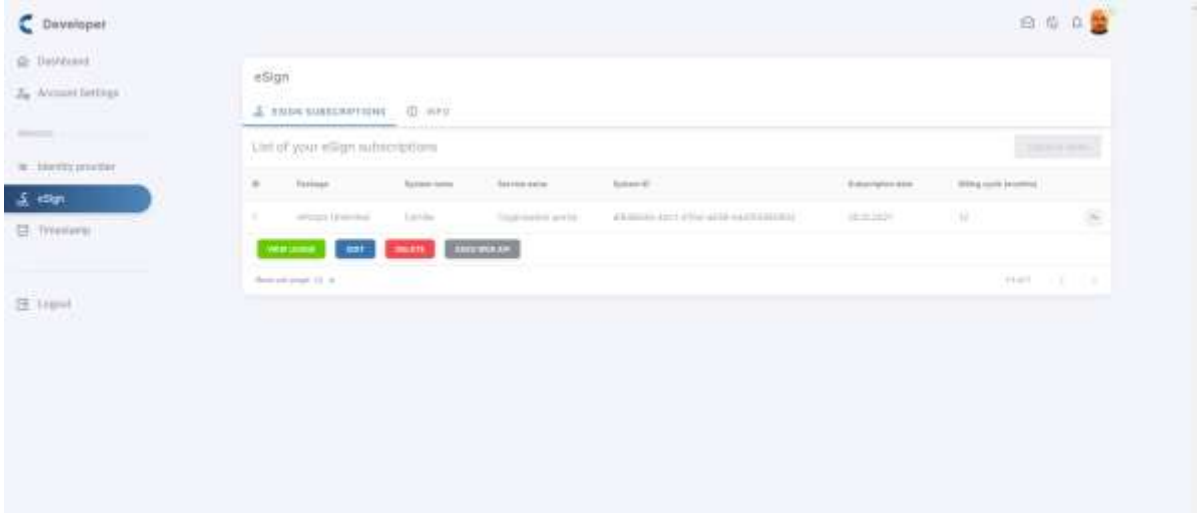

Opisi svih grešaka dostupni su pozivom na url:

Protokol: HTTPS

URL:
[PROD]: https://api.certilia.com/pades/v2/errors
[TEST] : https://api.test.certilia.com/pades/v2/errors

HTTP Metoda: GET

Sigurnost: SSL(TLS1.2, TLS1.3)
Header: Authorization: Bearer TOKEN_VALUE
Napomena: TOKEN_VALUE je potrebno generirati putem Certilia Developer portala (https://developer.certilia.com), klikom na opciju ADES WEB API



5.3.7.2 XAdES

Primjeri:


```
"Version": "XAdES-Certilia,15.03.2024. 13:00:52",
  "Note": "For PAdES/XAdES/nAdES.",
  "Platforms": "Certilia, MU_SDURD.",
  "SampleErrorMessages": [
    "{ Error = { Type = HG_INSUFFICIENT_PRIVILEGES, Code = 75, Message = INVALID_PERSON_NAME_SURNAME, Description = Nedozvoljeni pristup. } }",
    "{ Error = { Type = HG_INSUFFICIENT_PRIVILEGES, Code = 75, Message = INVALID_PERSON_NAME_SURNAME, Description = Invalid person's name and surname. } }",
    "{ Error = { Type = HG_INVALID_REQUEST, Code = 76, Message = INVALID_PERSON_PIN, Description = Neispravan OIB osobe. } }",
    "{ Error = { Type = HXML_INTERNAL_ERROR, Code = 7304, Message = INVALID_XML_SIGNATURE_ELEMENT, Description = Neispravan xml element koji sadrži potpis. } }",
    "{ Error = { Type = HXML_INTERNAL_ERROR, Code = 7303, Message = INVALID_XML_OBJECT, Description = Neispravan xml objekt ili referenca. } }",
    "{ Error = { Type = HG_INVALID_REQUEST, Code = 750, Message = UNSUPPORTED_SIGNATURE_LEVEL, Description = Invalid eIDAS signature level. } }",
    "{ Error = { Type = HG_INVALID_REQUEST, Code = 780, Message = INVALID_SIGNATURE_VALUE, Description = Invalid signature value. } }",
    "{ Error = { Type = HG_INVALID_REQUEST, Code = 716, Message = INVALID_VERIFICATION_CODE, Description = Invalid or duplicate verification code. } }",
    "{ Error = { Type = HG_INVALID_REQUEST, Code = 760, Message = INVALID_TSA_URL, Description = Neispravan URL TSA servisa. } }",
    "{ Error = { Type = HL_INVALID_AUTHORIZATION_CREDENTIALS, Code = 764, Message = INVALID_TSA_CREDENTIALS, Description = Neispravni autorizacijski podaci. } }",
    "{ Error = { Type = HS_INVALID_SIGNATURE_DATA, Code = 781, Message = SIGNATURE_NOT_VERIFIED, Description = Neuspješna verifikacija potpisa. } }",
    "{ Error = { Type = HUC_INVALID_USER_CERTIFICATE, Code = 777, Message = USER_CERTIFICATE_EXPIRED, Description = Korisnički certifikat je istekao. } }",
    "{ Error = { Type = HG_INVALID_REQUEST, Code = 710, Message = INVALID_ORGANIZATION_NAME, Description = Invalid organzation's name. } }",
    "{ Error = { Type = HG_INVALID_REQUEST, Code = 711, Message = INVALID_ORGANIZATION_VAT, Description = Invalid organzation's VAT. } }",
    "{ Error = { Type = HG_INVALID_REQUEST, Code = 710, Message = INVALID_ORGANIZATION_NAME, Description = Neispravan naziv organizacije. } }",
    "{ Error = { Type = HG_INVALID_REQUEST, Code = 711, Message = INVALID_ORGANIZATION_VAT, Description = Neispravan OIB organizacije. } }"
  ]
```

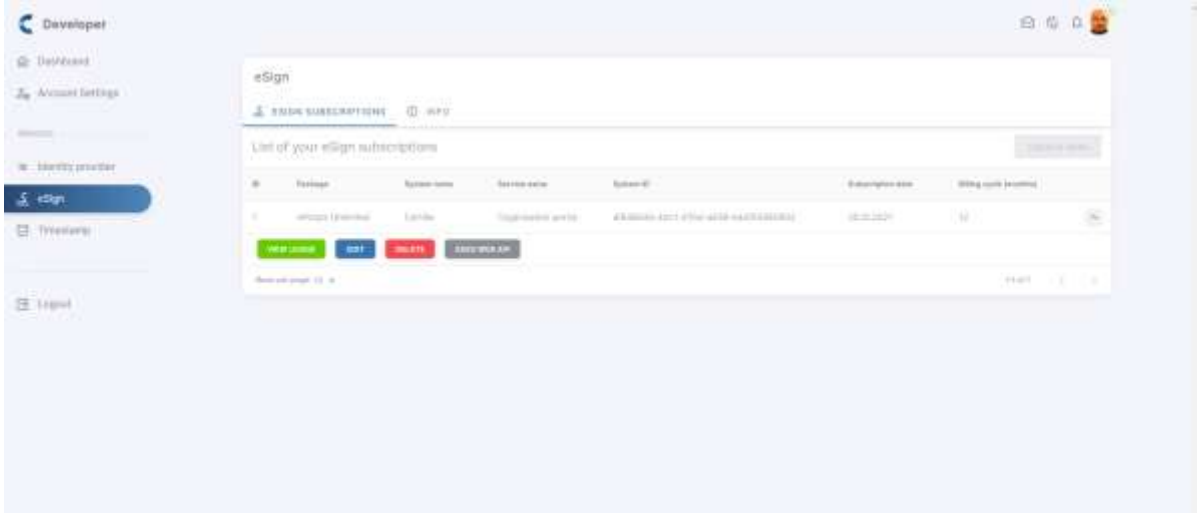

Opisi svih grešaka dostupni su pozivom na url:

Protokol: HTTPS

URL:
[PROD]: https://api.certilia.com/xades/v1/errors
[TEST] : https://api.test.certilia.com/xades/v1/errors

HTTP Metoda: GET

Sigurnost: SSL(TLS1.2, TLS1.3)
Header: Authorization: Bearer TOKEN_VALUE
Napomena: TOKEN_VALUE je potrebno generirati putem Certilia Developer portala (https://developer.certilia.com), klikom na opciju ADES WEB API



Stranica namjerno ostavljena prazna.

6 Prilozi

6.1 Prilog A – Lokacije vizualnog elementa unutar A4 stranice

Mreža za lokaciju vizuala unutar stranice izračunava se dinamički ovisno o veličini stranice i za svaki pojedini dokument, prema sljedećim parametrima:

- Pročita se veličina stranice na kojoj se želi dodati potpis, npr. rectangle **pageSize** ={X = 0 Y = 0 Width = 612 Height = 792}
- Veličina vizuala je zadana:
    - za standardni vizual
        - rectangle **visualSize** = {X = 0 Y = 0 Width = 248 Height = 122}
    - za vizual 'small'
        - rectangle **visualSize** = {X = 0 Y = 0 Width = 248 Height = 61}
- Varijabla za pretvorbu dimenzija double **pointsInmm** = 2.83464567
- Metoda za izračun mreže lokacija dana je u nastavku.
    - Pomoću metode moguće je za veličinu stranice u dokumentu predvidjeti točnu lokaciju na koju će se ugraditi vizual prema zadanoj relativnoj lokaciji (parametar pageLocation, poglavlje 5.3.5) unutar stranice - **RelPos**)
    - Pomoću metode može se npr.: prije poziva POST metode (PreSign) u aplikaciji korisnika vizualizirati točna lokacija vizuala unutar zadane stranice, točno onako kako će isti biti ugrađen u potpisani dokument.

Metoda za izračun mreže lokacija vizuala za zadanu veličinu stranice:

```
private Tuple<List<VisualSignatureGrid>, int, int> GetVisualGrid(Rectangle pageSize, Rectangle visualSize)
        {
            int col = 0;
            int row = 0;
            doublepointsInmm = 2.83464567;
            List<VisualSignatureGrid> grid = new List<VisualSignatureGrid>();
            float marginPageH = 10 * (float)pointsInmm;
            float marginPageV = 10 * (float)pointsInmm;
            int horizCount = Convert.ToInt32(Math.Floor((pageSize.Width-(2*marginPageH)) / visualSize.Width));
            int vertCount;

            if (horizCount>0)
            {
                vertCount = Convert.ToInt32(Math.Floor((pageSize.Height-(2*marginPageV)) / visualSize.Height));
                if (vertCount>0)
                {
                    float horizSpaceAv = pageSize.Width - ((2 * marginPageH) + (horizCount * visualSize.Width));
                    float vertSpaceAv = pageSize.Height - ((2 * marginPageV) + (vertCount * visualSize.Height));

                    float horizSpace = horizSpaceAv / (horizCount-1);
                    float vertSpace = vertSpaceAv / (vertCount-1);

                    int cnt = 1;
                    float bottomStart = pageSize.Height - marginPageV-visualSize.Height;
                    for (col=1; col<=vertCount;col++)
                    {
                        float leftStart = marginPageH;
                        for (row=1; row<=horizCount;row++)
                        {
                            float pLeft = leftStart;
                            float pBottom = bottomStart;

                            grid.Add(new VisualSignatureGrid
                            {
                                RelPos = cnt,
                                PosX = col, PosY = row,
                                Left = pLeft, Bottom = pBottom
                            });
                            leftStart = leftStart + horizSpace + visualSize.Width;
                            cnt++;
                        }
                        bottomStart = bottomStart - vertSpace - visualSize.Height;
                    }
                }
            }
            return Tuple.Create(grid,col-1,row-1);
        }
```

U nastavku je prikaz lokacija za stranicu veličine A4, orijentacija portrait te orijentacije landscape (Napomena: Prikaz ne sadrži stvarne margine).

Vrijednosti **pageLocation** varijable za pozicioniranje standardnog vizualnog elementa na A4 stranici (Portrait):

1	2
3	4
5	6
7	8
9	10
11	12

Vrijednosti **pageLocation** varijable za pozicioniranje vizualnog elementa '**small**' na A4 stranici (Portrait):

1	2
3	4
5	6
7	8
9	10
11	12
13	14
15	16
17	18
19	20
21	22
23	24

Vrijednosti **pageLocation** varijable za pozicioniranje standardnog vizualnog na stranici veličine A4 (Landscape):

1	2	3
4	5	6
7	8	9
10	11	12

Vrijednosti **pageLocation** varijable za pozicioniranje vizualnog elementa ('**small**') na stranici veličine A4 (Landscape):

1	2	3
4	5	6
7	8	9
10	11	12
13	14	15
16	17	18
19	20	21
22	23	24
25	26	27

6.2 Prilog B – Elementi standardnog vizuala



Slika B: Elementi standardnog vizuala

Tablica 6.2 Elementi standardnog vizuala

	Element	Vidljivost	Napomene
1	Ime i prezime potpisnika/Naziv pečata	Uvijek, naziv pečata opcionalno	Kod pečata se ovdje ispisuje naziv pečata ako je specificiran.
2	PIN (OIB) potpisnika	Uvijek	Kod pečata se ovdje ispisuje VAT organizacije.
3	Naziv organizacije	Opcionalno	Kod potpisa, ako je zadan parametar organizationName.
4	Datum i vrijeme potpisa/pečata***	Uvijek	Kod potpisivanja se ispisuje Elektronički potpisano. Kod pečatiranja se ispisuje Elektronički pečatirano.
5	Izdavatelj certifikata	Uvijek	Ne koristi se.
6	Link za provjeru izvršenog potpisa	Uvijek	Transakciju evidentira ePotpis (datum i vrijeme transakcije te uspješno ili neuspješno potpisivanje).
7	Broj zapisa	Uvijek	Verification code.
8	Poruka e-Usluge redak 1	Opcionalno	Max 60 znakova.
9	Poruka e-Usluge redak 2	Opcionalno	Max 60 znakova.
10	Poruka e-Usluge redak 3	Opcionalno	Max 60 znakova.
11	QR kod za provjeru potpisa putem mobilnih uređaja	Uvijek	U QR kodu se nalaze elementi pod r.br. 6 i 7.

**** Datum i vrijeme potpisa ne moraju odgovarati točnom trenutku potpisa (potpis se kreira nakon unosa PIN-a privatnog ključa), vidi 5.3.4.2.*

Napomena: U određenim slučajevima moguća su manja odstupanja u pozicijama/vrijednostima od gore navedenog opisa.

6.3 Prilog C – Elementi vizuala 'small'



Slika C: Elementi vizuala 'small'

Koriste se elementi kao i za standardni vizual, navedeni u prilogu B - osim elementa 5, 6, 7, 8, 9 i 10.