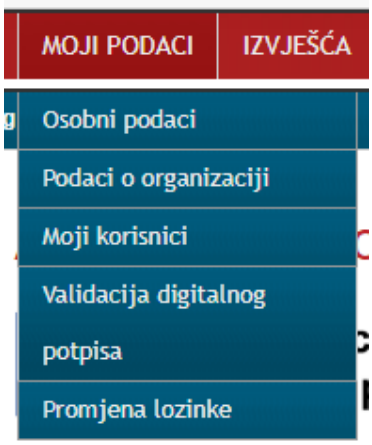
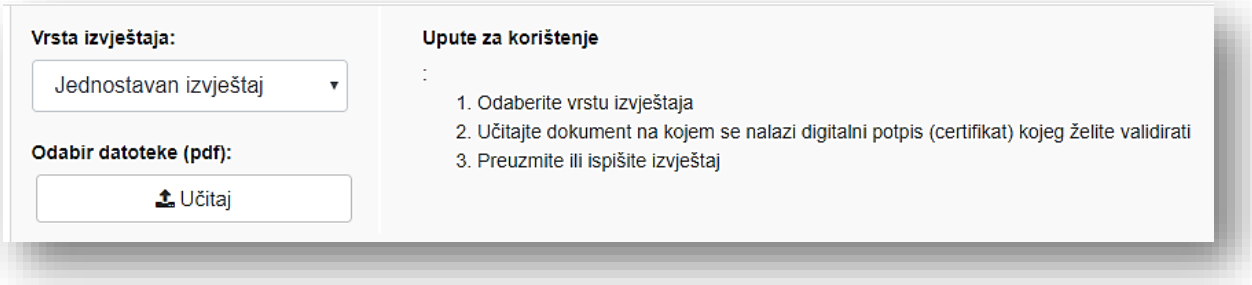
Alat za validaciju digitalnih potpisa – provjera od strane naručitelja

Alat za validaciju digitalnih potpisa

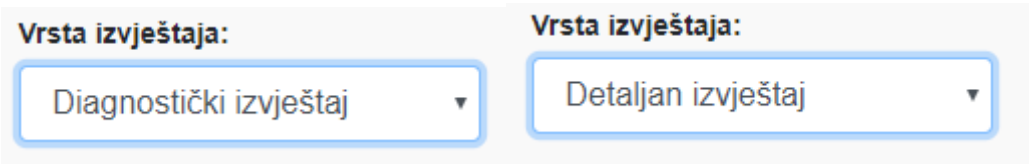
Sufinancirano instrumentom Europske unije za povezivanje Europe

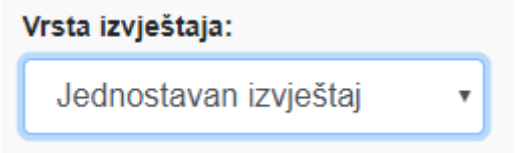
Korak 1. Odabir alata



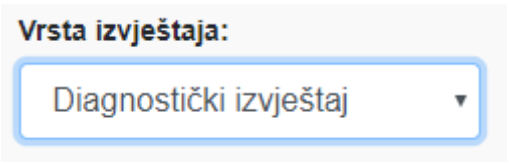


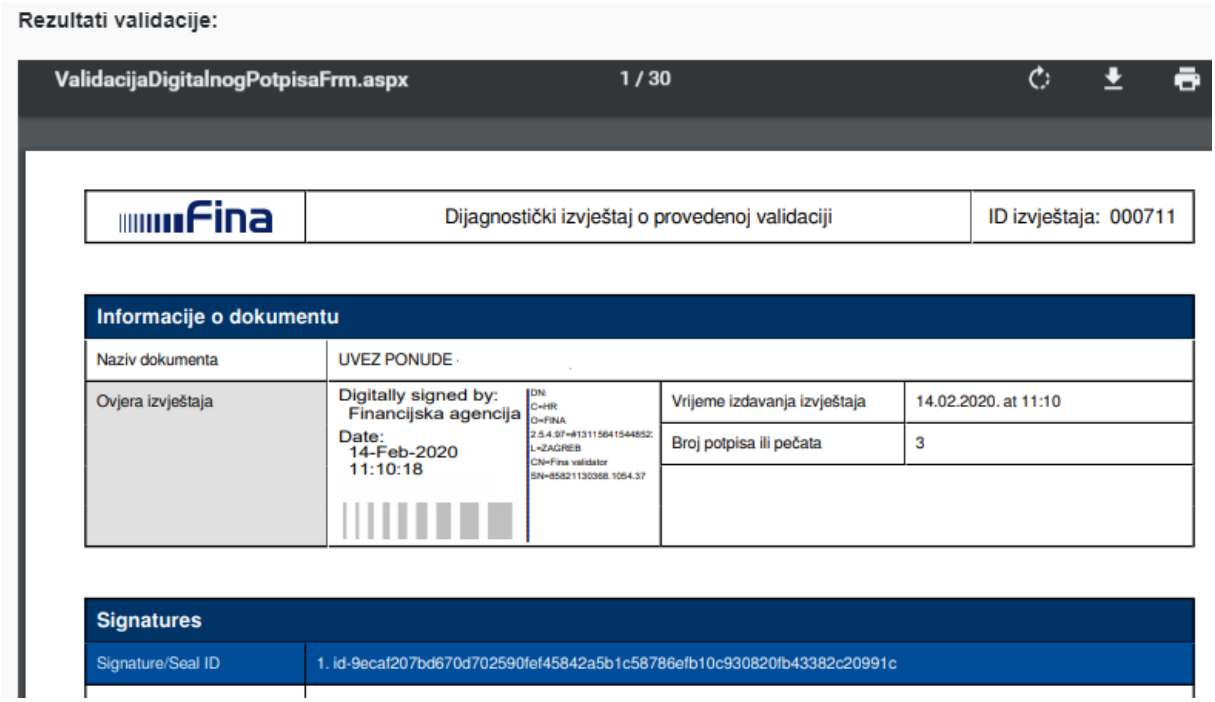
Korak 2. Vrste izvještaja za odabir





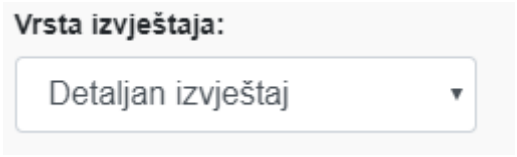
Korak 2.1. Odabir Dijagnostičkog izvještaja s rezultatima provjere





Certificate Chain	Source	TRUSTED_LIST
	ID	2340A9E8D61E84EF3A08A940F61A206A0AACA3401575F0DB7DDD59
	Source	TRUSTED_LIST
	ID	857BFCE43B1BB4601FF4543B46D3FB2E213BF9B4FEEB6F13BE9EF45

Korak 2.2. Odabir Detaljnog izvještaja s rezultatima provjere



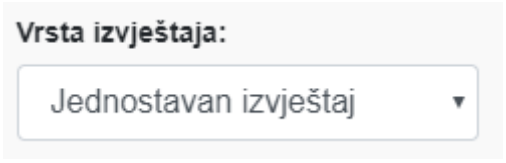
ValidacijaDigitalnogPotpisaFrm.aspx 1 / 12

Informacije o potpisu ili pečatu	
ID potpisa ili pečata	1. id-9ecaf207bd670d702590fef45842a5b1c58786efb10c930820fb4
Postupak validacije za osnovne potpise	
Je li rezultat osnovnog validacijskog postupka konačan?	NIJE OK
Zaključak:	NEODREĐENO
Postupak validacije za vremenske žigove	
0D2B19B209A14783E4914AD99B872F3FBBBC7B5B783DEC46FFEE2	
Je li rezultat postupka validacije vremenskih žigova konačan?	OK
Zaključak:	USPJEŠNO
Postupak validacije za potpise s vremenom te potpise s podacima o dugoročnoj validaciji	
Je li rezultat osnovnog validacijskog postupka prihvatljiv?	OK
Je li rezultat postupka validacije podataka o opozvanosti certifikata prihvatljiv?	OK
Je li najbolje vrijeme potpisa (best-signature-time) nakon datuma izdavanja potpisnog certifikata?	OK
Zaključak:	NEODREĐENO
Postupak validacije za potpise s arhivskim podacima	
Je li rezultat postupka LTV validacije prihvatljiv?	OK
Je li validacija potpisa za trenutak iz prošlosti konačna?	NIJE OK
Zaključak:	NEODREĐENO
Kvalifikacija potpisa: QESig	

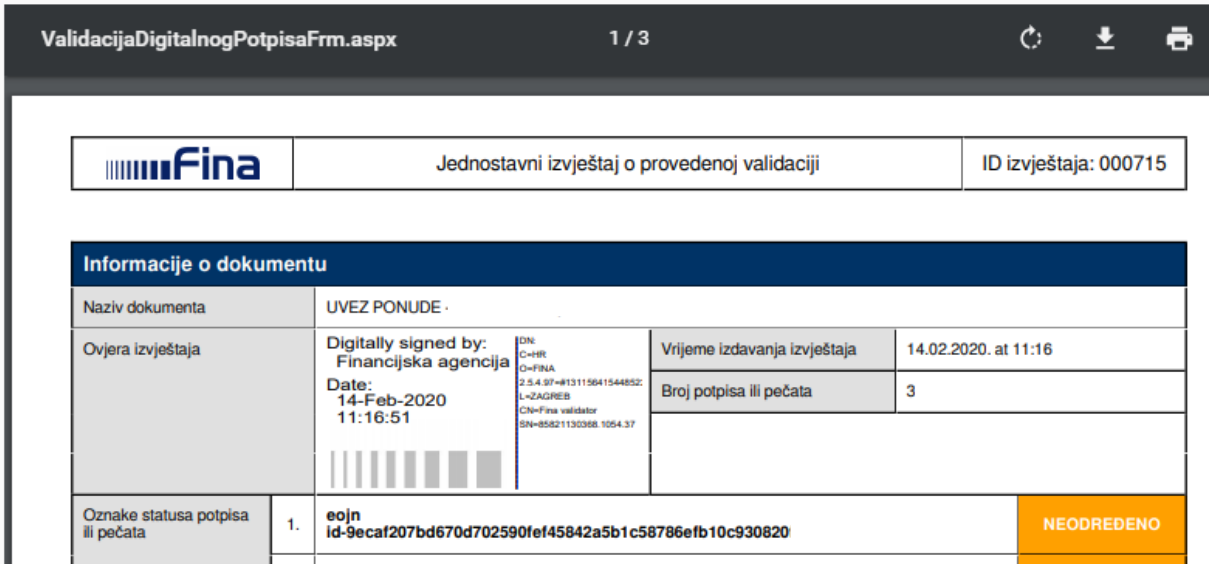
OPOZIV	d81b0cb081eedee6a982d663c5787b131dafaaad3dc7555a16d5b2e93719f7215b7447ba56b1a0a33f9c51e4631519434a8e598659e818c131
Identifikacija potpisnog certifikata	USPJEŠNO
Postoji li kandidat prepoznat kao potpisni certifikat?	OK
Kriptografska verifikacija	USPJEŠNO
Je li potpis nepromijenjen i neoštećen?	OK
Validacija prihvatljivosti potpisa	USPJEŠNO
Jesu li zadovoljena kriptografska ograničenja potpisa?	OK
Validacija X509 certifikata	USPJEŠNO
Može li se izgraditi lanac certifikata do uporišta povjerenja („trust anchor“)?	OK
Je li validacija certifikata konačna?	OK
Je li validacija certifikata konačna?	OK
Certifikat id-4EE0DA0EEFBFAE2BD4E3ADD051E1CA9A9EDFEEE74682EBBB074	USPJEŠNO
Je li potpis certifikata nepromijenjen i neoštećen?	OK

POTPIS	id-9ecaf207bd670d702590fef45842a5b1c58786efb10c930820fb43
Provjera formata	USPJEŠNO
Je li pronađen očekivani format?	OK
Identifikacija potpisnog certifikata	USPJEŠNO
Postoji li kandidat prepoznat kao potpisni certifikat?	OK
Inicijalizacija konteksta validacije	USPJEŠNO
Jesu li poznata pravila potpisivanja?	OK
Kriptografska verifikacija	USPJEŠNO
Je li pronađen objekt referentnih podataka?	OK
Je li objekt referentnih podataka nepromijenjen i neoštećen?	OK
Je li potpis nepromijenjen i neoštećen?	OK
Validacija prihvatljivosti potpisa	USPJEŠNO
Postoji li potpisano kvalificirajuće svojstvo „signing-time“?	OK
Jesu li zadovoljena kriptografska ograničenja potpisa?	OK

Korak 2.3. Odabir Jednostavnog izvještaja s rezultatima provjere i obrazloženjem



Rezultati validacije:



ID potpisa ili pečata	3. id-bb4a82792f1cde656601cb7209ea410b136b84950c7affdee00945
Razina potpisa ili pečata	Napredan elektronički potpis s nepotpunim rezultatom provjere[15]
Oznaka statusa	NEODREDENO[16]
Pojašnjenje statusa	NO_POE
Greške	Validacija potpisa za trenutak iz prošlosti nije konačna!
Upozorenja	Certifikat nije kvalificiran u vrijeme izdavanja! Privatni ključ se u vremenu izdavanja ne nalazi u QSCD-u! Certifikat nije kvalificiran u (najboljem) vremenu potpisivanja! Nalazi li se privatni ključ u QSCD-u u (najboljem) vremenu potpisivanja? Potpis/pečat je AdES s nepotpunim rezultatom provjere („INDETERMINATE AdES")! Certifikat potpisnika nema očekivanu specifikaciju uporabe ključa.
Format potpisa ili pečata	PKCS7-LT (Public Key Cryptography Standards #7 – Long Term Level)[17]
Lanac certifikata	eojn Fina RDC 2015 Fina Root CA

[1] *Napredan elektronički potpis čiji rezultat provjere zbog nedostatnih informacija dostupnih u trenutku provođenja validacije onemogućuje potpuno utvrđivanje konačne razine potpisa. Dio validacije koji se odnosi na provjeru formata i verifikaciju digitalnog potpisa uspješno je proveden.*

[2] *Zbog nedostatnih informacija dostupnih u trenutku provođenja validacije rezultati provedenih provjera onemogućuje potpuno utvrđivanje oznake statusa POTPUNO USPJEŠNO ili POTPUNO NEUSPJEŠNO.*

[3] *Polazišna verzija PKCS#7 digitalnog potpisa koji sadrži vremenski žig povezan s vremenom potpisivanja te certifikate i pripadajuće podatke o opozivu kako bi se omogućila verifikacija potpisa u budućnosti, čak i ako dohvaćanje podataka o opozivu s originalnog izvora više ne bi bilo moguće. U ovaj se digitalni potpis može pouzdati kroz dulje vremensko razdoblje (npr. vremensko razdoblje koje je dulje u odnosu na period valjanosti potpisnog certifikata).*

[4] *Utvrđeno vrijeme izrade potpisa ili pečata.*

[5] *Najranije vrijeme u kojem postoji dokaz postojanja potpisa.*

[6] *Dokument može biti potpisan ili pečatiran s jednim ili više potpisa ili pečata, a pojam pozicija potpisa određuje pojedini potpis ili pečat koji je validiran u okviru ovog ID potpisa ili pečata.*

[7] *Opseg dokumenta koji je obuhvaćen potpisom.*

[8] *Napredan elektronički potpis čiji rezultat provjere zbog nedostatnih informacija dostupnih u trenutku provođenja validacije onemogućuje potpuno utvrđivanje konačne razine potpisa. Dio validacije koji se odnosi na provjeru formata i verifikaciju digitalnog potpisa uspješno je proveden.*

[9] *Zbog nedostatnih informacija dostupnih u trenutku provođenja validacije rezultati provedenih provjera onemogućuje potpuno utvrđivanje oznake statusa POTPUNO USPJEŠNO ili POTPUNO NEUSPJEŠNO.*

[10] *Polazišna verzija PKCS#7 digitalnog potpisa koji sadrži vremenski žig povezan s vremenom potpisivanja te certifikate i pripadajuće podatke o opozivu kako bi se omogućila verifikacija potpisa u budućnosti, čak i ako dohvaćanje podataka o opozivu s originalnog izvora više ne bi bilo moguće. U ovaj se digitalni potpis može pouzdati kroz dulje vremensko razdoblje (npr. vremensko razdoblje koje je dulje u odnosu na period valjanosti potpisnog certifikata).*

[11] *Utvrđeno vrijeme izrade potpisa ili pečata.*

[12] *Najranije vrijeme u kojem postoji dokaz postojanja potpisa.*

[13] *Dokument može biti potpisan ili pečatiran s jednim ili više potpisa ili pečata, a pojam pozicija potpisa određuje pojedini potpis ili pečat koji je validiran u*

[13] *Dokument može biti potpisan ili pečatiran s jednim ili više potpisa ili pečata, a pojam pozicija potpisa određuje pojedini potpis ili pečat koji je validiran u okviru ovog ID potpisa ili pečata.*

[14] *Opseg dokumenta koji je obuhvaćen potpisom.*

[15] *Napredan elektronički potpis čiji rezultat provjere zbog nedostatnih informacija dostupnih u trenutku provođenja validacije onemogućuje potpuno utvrđivanje konačne razine potpisa. Dio validacije koji se odnosi na provjeru formata i verifikaciju digitalnog potpisa uspješno je proveden.*

[16] *Zbog nedostatnih informacija dostupnih u trenutku provođenja validacije rezultati provedenih provjera onemogućuje potpuno utvrđivanje oznake statusa POTPUNO USPJEŠNO ili POTPUNO NEUSPJEŠNO.*

[17] *Polazišna verzija PKCS#7 digitalnog potpisa koji sadrži vremenski žig povezan s vremenom potpisivanja te certifikate i pripadajuće podatke o opozivu kako bi se omogućila verifikacija potpisa u budućnosti, čak i ako dohvaćanje podataka o opozivu s originalnog izvora više ne bi bilo moguće. U ovaj se digitalni potpis može pouzdati kroz dulje vremensko razdoblje (npr. vremensko razdoblje koje je dulje u odnosu na period valjanosti potpisnog certifikata).*

[18] *Utvrđeno vrijeme izrade potpisa ili pečata.*

[19] *Najranije vrijeme u kojem postoji dokaz postojanja potpisa.*

[20] *Dokument može biti potpisan ili pečatiran s jednim ili više potpisa ili pečata, a pojam pozicija potpisa određuje pojedini potpis ili pečat koji je validiran u okviru ovog ID potpisa ili pečata.*

[21] *Opseg dokumenta koji je obuhvaćen potpisom.*