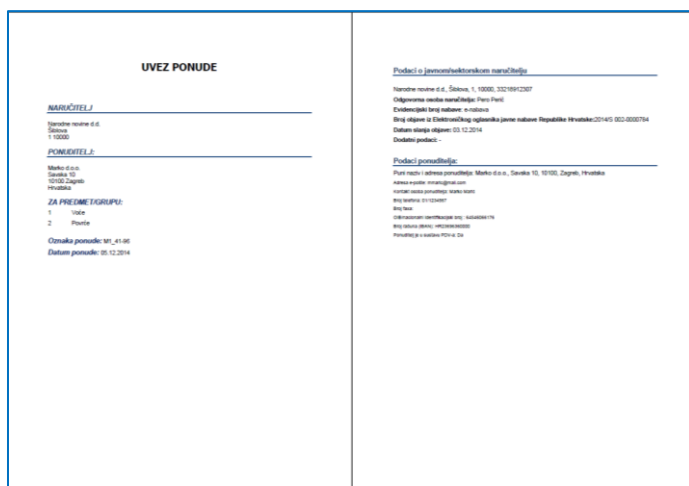
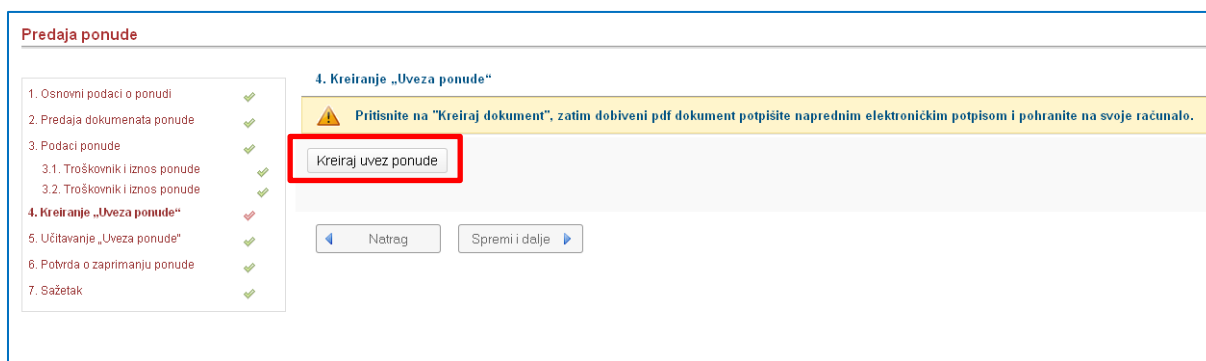


## e-nabava

### Kriptografska zaštita elektroničke ponude - Uveza ponude

#### „Uveza ponude“

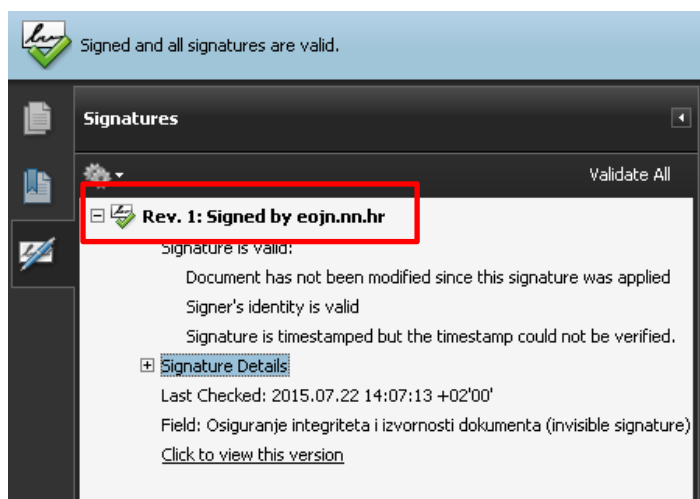
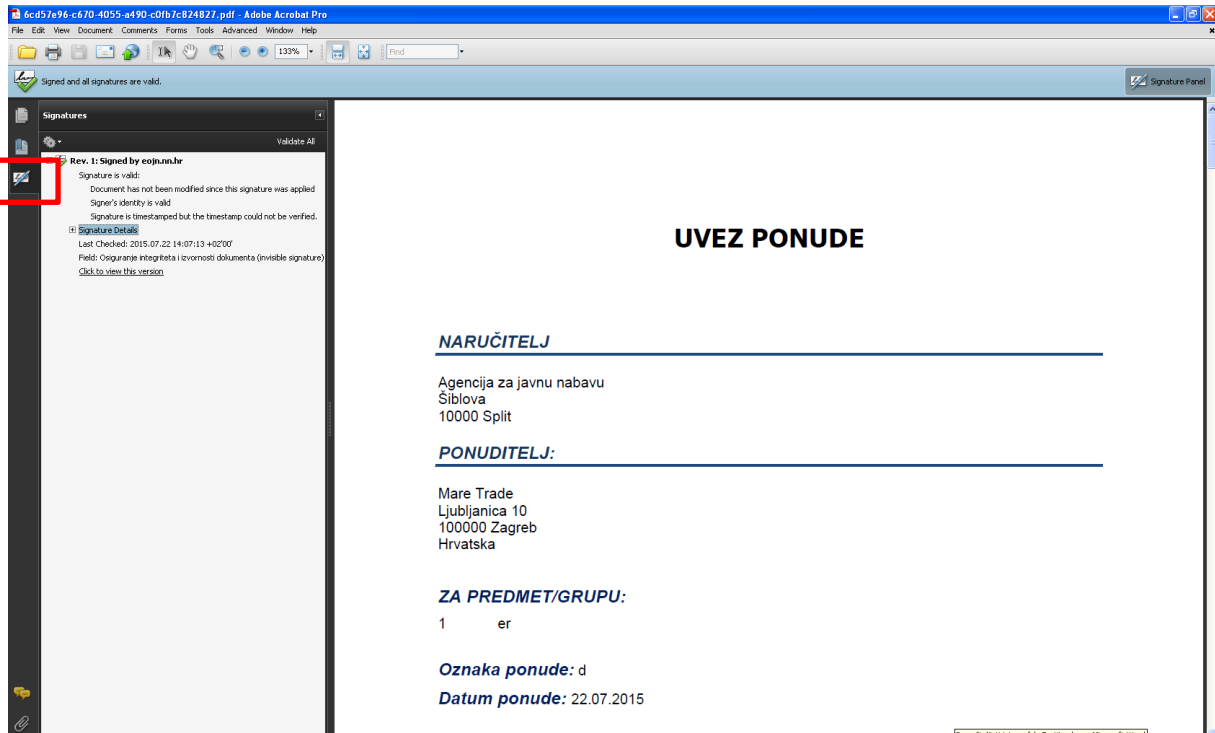
Uveza ponude je dokument (pdf) koji se generira iz sustava te sadrži sve podatke relevantne za predaju ponude na temelju unesenih informacija i datoteka. Uvezu ponude nije moguće mjenjati sadržaj i strukturu. **Uveza ponude sadrži onoliko ponudbenih listova za koliko se grupa predmeta nabave predala ponuda.** Uveza ponude sadrži XML vezu na dokumente ponude ukoliko su uploadani kao sastavni dijelovi cjelokupne ponude. Na taj način osigurana je konzistencija i integritet predane ponude.



## Pregled digitalnih potpisa koji se nalaze na kreiranom Uvezu ponude

Nakon što je Uvez ponude kreiran, na njemu se nalazi prvi potpis koji sugerira da je dokument Uvezu ponude kreiran iz sustava EOJN-a.

Provjeru digitalnih potpisa na dokumentu u Adobe programu provjeravate klikom na ikonu 



Kreirani Uvez ponude ne smije se modificirati tj. nisu dopuštene sljedeće aktivnosti

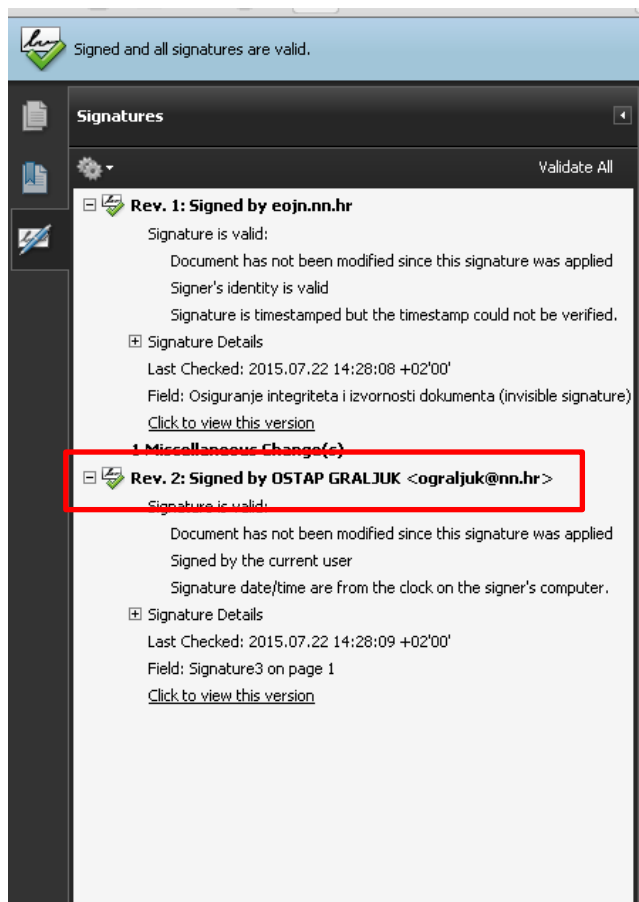
- zaključavati dokument lozinkama od strane samog korisnika
- mijenjati format dokumenta
- mijenjati sadržaj na samom dokumentu
- sažimati (komprimirati) kreirani Uvez ponude – zip ili rar format

Ukoliko biste modificirali Uvez ponude i takav Uvez ponude predali (uploadali), navedeni Uvez ponude neće zadovoljiti validaciju integriteta ponudbenog lista tj. sustav neće jamči za ispravnost podataka koji se nalaze na njemu.

Prije predaje (uploada) Uveza ponude potrebno ga je potpisati naprednim elektroničkim potpisom.

Nakon što ste ga digitalno potpisali naprednim elektroničkim potpisom, dokument Uveza ponude sadržava i drugi potpis – potpis ponuditelja.

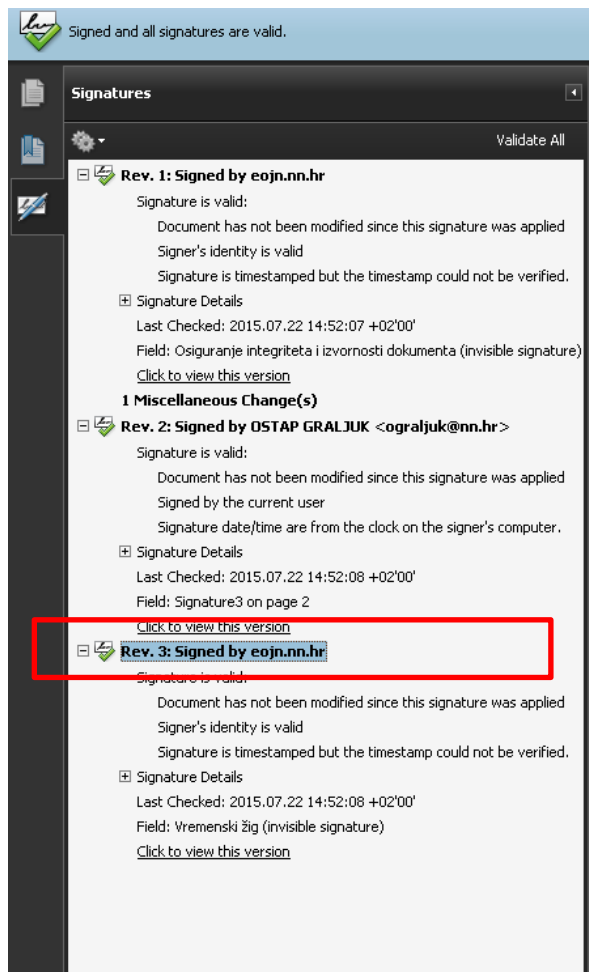
Uvez ponude također nije dopušteno modificirati nakon što je digitalno potpisan naprednim elektroničkim potpisom od strane ponuditelja.



Digitalno potpisani Uvez ponude se predaje (uploada) na sustav. Nakon predaje (uploada) potrebno je potvrditi da li se želi predati navedna ponuda te se potvrdom slanja smatra trenutak dostave elektroničke ponude.

Također se zaprima informacija, na registrirani e-mail korisnika, obavijest o predanoj elektroničkoj ponudi.

U trenutku predaje (uploada) ponude tj. Uveza ponude, navedeni dokument dobiva i treći potpis – vremenski žig.



Vremenski žig je elektronički potpisana potvrda izdavatelja koja potvrđuje sadržaj podataka na koje se odnosi u navedenom vremenu. Vremenski žig predstavlja skup informacija o vremenu njegovog apliciranja na pojedini dokument. Stavljanje vremenskog žiga izvodi se kod Fine, kao Time Stamp Authority (TSA) koja je pružatelj usluge.

Važno je napomenuti da se u trenutku predaje ponude, uvez ponude kriptira mehanizmom koji je ugrađen u sustav te nije moguće ostvariti uvid u bilo koji element ponude, sve do procesa javnog otvaranja ponuda, gdje se pristigle ponude validiraju te potom pohranjuju u sustav. Drugim rječima, dok nije istekao rok za podnošenje ponude i započelo javno otvaranje, nije moguće dekriptirati odnosno omogućiti uvid u bilo koji dio ponude a samim time i uvid u dokument Uvez ponude.

## Mehanizmi kriptiranja

*Enkripcija* je proces transformacije informacija korištenjem algoritama na način da učini informaciju / dokument nečitljivim bilo kojem subjektu osim onom koji posjeduje specifičan ključ. Rezultat procesa je enkriptirana informacija odnosno dokument.

*Dekripcija* predstavlja suprotan proces od enkripcije – proces transformacije informacija (dokumenata) iz nečitljivog u čitljivu, originalnu informaciju – dokument, korištenjem predefiniranog algoritma i odgovarajućeg ključa.

U e-dostavi koristi se hibridni kriptosustav koji koristi simetričnu i asimetričnu kriptografsku metodu:

- Simetričnu kriptografiju za enkripciju dokumenata
- Asimetričnu kriptografiju za enkripciju/dekripciju ključa koji se koristi za simetričnu enkripciju/dekripciju

## Asimetrična kriptografija

Asimetrična kriptografija je kriptografski sustav koji zahtjeva par ključeva za procese enkripcije i dekripcije :

- Privatni ključ (dostupan na pojedincu)
- Javni ključ (dostupan bilo kojoj zainteresiranoj strani)

Par ključeva ima svojstvo da ako jedan ključ iz para kriptira poruku, tada isključivo drugi ključ iz para može dekriptirati poruku. U procesu e-dostave kriptiranje se obavlja javnim ključevima ovlaštenih predstavnika (dvostruko kriptiranje), a dekriptiranje privatnim ključevima ovlaštenih predstavnika.

## Simetrična kriptografija

Simetrična kriptografija je kriptografski sustav koji omogućava procese enkripcije/dekripcije informacija dokumenata korištenjem jednog te istog ključa za oba procesa.

## Provjere koje sustav EOJN-a vrši na elektronički dostavljenoj ponudi/zahtjevu za sudjelovanje

Prilikom predaje Uveza ponude odnosno Uveza zahtjeva za sudjelovanje ili na javnom otvaranju ponuda tj. otvaranju Zahtjeva za sudjelovanje sustav provjerava navedene dokumente po sljedećim točkama

Provjera izvornosti uveza ponude (čl. 27., st. 1., čl. 28., st. 1. Uredbe o načinu izrade i postupanju s dokumentacijom za nadmetanje i ponudama – NN 10/2012), čl. 8., st. 6., Zakona o izmjenama i dopuna Zakon o javnoj nabavi – NN 83/2013	✓
Postojanje naprednog elektroničkog potpisa (čl. 8., st. 4., točka 4. Zakona o izmjenama i dopuna Zakona o javnoj nabavi – NN 83/2013)	✓
Provjera vremenskog žiga na „Uvezu ponude“ (čl. 29., st. 1. Uredbe o načinu izrade i postupanju s dokumentacijom za nadmetanje i ponudama – NN 10/2012)	✓
Utvrdjivanje ispravnosti naprednog elektroničkog potpisa (čl. 30., st. 2. Uredbe o načinu izrade i postupanju s dokumentacijom za nadmetanje i ponudama – NN 10/2012)	✓
Provjera cjelovitosti „Uveza ponude“ (čl. 27., st. 2. Uredbe o načinu izrade i postupanju s dokumentacijom za nadmetanje i ponudama – NN 10/2012)	✓
Provjera cjelovitosti cjelokupne ponude (čl. 27., st. 2. Uredbe o načinu izrade i postupanju s dokumentacijom za nadmetanje i ponudama – NN 10/2012)	✓
Pravodobno podnesena ponuda (čl. 29., st. 3. Uredbe o načinu izrade i postupanju s dokumentacijom za nadmetanje i ponudama – NN 10/2012)	✓

- *Provjera izvornosti uveza ponude (čl. 27., st. 1., čl. 28., st. 1. Uredbe o načinu izrade i postupanju s dokumentacijom za nadmetanje i ponudama – NN 10/2012), čl. 8., st. 6., Zakona o izmjenama i dopuna Zakon o javnoj nabavi – NN 83/2013 – da li je predani dokument kreiran od strane samog sustava EOJN-a*
- *Postojanje naprednog elektroničkog potpisa (čl. 8., st. 4., točka 4. Zakona o izmjenama i dopuna Zakona o javnoj nabavi – NN 83/2013) – da li je ponuditelj potpisao priloženi dokument naprednim elektroničkim potpisom*
- *Provjera vremenskog žiga na „Uvezu ponude“ (čl. 29., st. 1. Uredbe o načinu izrade i postupanju s dokumentacijom za nadmetanje i ponudama – NN 10/2012) – da li priloženi dokument ima potpis vremenskog žiga*
- *Utvrdjivanje ispravnosti naprednog elektroničkog potpisa (čl. 30., st. 2. Uredbe o načinu izrade i postupanju s dokumentacijom za nadmetanje i ponudama – NN 10/2012) – da li je certifikat na digitalnom potpisu ponuditelja ispravan tj. valjan (da li se nalazi „EU Trusted Lists of Certification Service Provider“ )*  
<https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers>
- *Provjera cjelovitosti „Uveza ponude“ (čl. 27., st. 2. Uredbe o načinu izrade i postupanju s dokumentacijom za nadmetanje i ponudama – NN 10/2012) – da li je predani priloženi dokument (ponudbeni list/ZZS) naknadno modificiran*

- *Provjera cjelovitosti cjelokupne ponude (čl. 27., st. 2. Uredbe o načinu izrade i postupanju s dokumentacijom za nadmetanje i ponudama – NN 10/2012) – da li su priloženi dokumenti ponude/ZZS-a sastavni dio te ponude odnosno zahtjeva tj. da li se učitava Uvez ponude koji je sustav kreirao za navedeni postupak*
- *Pravodobno podnesena ponuda (čl. 29., st. 3 Uredbe o načinu izrade i postupanju s dokumentacijom za nadmetanje i ponudama – NN 10/2012) – da li je priloženi dokument priložen na sustav prije isteka roka za dostavu ponuda/ZZS-a*