



Naziv projekta: e-Poslovanje

UP.04.1.1.16.0001

PROJEKTNA DOKUMENTACIJA

„Tehnička specifikacija za integraciju web registracijskog obrasca za
dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja“

PARTNER

Financijska agencija

Datum:

Veljača, 2024.

Projekt je sufinancirala Europska Unija iz Europskog socijalnog fonda.

Sadržaj dokumenta isključiva je odgovornost Središnjeg državnog ureda za razvoj digitalnog društva.

Središnji državni ured za razvoj digitalnog društva	Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja		
	Projekt: e-Poslovanje	Komponenta: e-Ovlaštenja	Djelokrug: FINA
	Datum: 19.02.2024.	Namjena: Za dionike u projektu	Verzija: 2.3

Projekt e-Poslovanje

Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja

Središnji državni ured za razvoj digitalnog društva	Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja		
	Projekt: e-Poslovanje	Komponenta: e-Ovlaštenja	Djelokrug: FINA
	Datum: 19.02.2024.	Namjena: Za dionike u projektu	Verzija: 2.3

SADRŽAJ:

1. Uvod	5
2. Preuvjeti za integraciju pružatelja e-usluga	6
2.1 Dijagram tijeka komunikacije	7
2.2 Specifikacija protokola	9
2.2.1 HTTP Redirect Binding protokol.....	9
2.2.2 HTTP POST metoda.....	10
2.3 Specifikacija poruka	10
2.3.1 ServiceRequest.....	10
2.3.2 ServiceResponse	16
2.4 Specifičnosti za pružatelje e-usluga	19
2.5 Sigurnost	20

Središnji državni ured za razvoj digitalnog društva	Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja		
	Projekt: e-Poslovanje	Komponenta: e-Ovlaštenja	Djelokrug: FINA
	Datum: 19.02.2024.	Namjena: Za dionike u projektu	Verzija: 2.3

Povijest promjena

Br.	Verzija	Opis	Datum	Autori
1.	0.1	Radna verzija - nacrt	25.06.2018.	Fina
2.	0.2	Izmjene kod atributa XSD-a	30.07.2018.	Fina
3.	2.0	Usklađivanje prema novoj strukturi JIPS-a	31.07.2019.	Fina
4.	2.1	Prilagodba terminologije	17.03.2020.	Fina
5.	2.2	Maknut Images element, dodan ValueDescription, Description postavljen kao obavezno polje	05.11.2020.	Fina
6.	2.3	Ažuriranje izvora i usklađivanje terminologije	19.02.2024.	Središnji državni ured za razvoj digitalnog društva

Središnji državni ured za razvoj digitalnog društva	Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja		
	Projekt: e-Poslovanje	Komponenta: e-Ovlaštenja	Djelokrug: FINA
	Datum: 19.02.2024.	Namjena: Za dionike u projektu	Verzija: 2.3

1. Uvod

Ovaj dokument ima svrhu definiranja tehničkih preduvjeta koje je nužno ispuniti da bi se ostvarila integracija pružatelja e-usluga s podsustavom e-Ovlaštenja sustava e-Poslovanja te ima svrhu specificiranja načina razmjene podataka između pružatelja e-usluga i e-Ovlaštenja, a sve u cilju sigurne razmjene podatka nužnih za proces kreiranja e-Punomoći.

Ovaj dokument opisuje tehničke zahtjeve potrebne za integraciju web obrasca za dodjelu prava korisnicima na e-Uslugu sa e-Ovlaštenjima, kao osnovni proces davanja e-Punomoći na uslugu.

Način dohvata i provjere e-Punomoći opisan je u dokumentu „Tehnička specifikacija za dohvat autorizacijskih podataka“.

Središnji državni ured za razvoj digitalnog društva	Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja		
	Projekt: e-Poslovanje	Komponenta: e-Ovlaštenja	Djelokrug: FINA
	Datum: 19.02.2024.	Namjena: Za dionike u projektu	Verzija: 2.3

2. Preduvjeti za integraciju pružatelja e-usluga

Svrha e-Ovlaštenja je da pružateljima e-usluga olakša autorizaciju korisnika na e-uslugu, tj. omogući im on-line dodjelu autorizacije (e-Punomoći) na uslugu. Usluga e-Ovlaštenja to omogućuje na način da jedna osoba „opunomoćitelj“ može dati drugoj osobi „opunomoćenik“ e-Punomoć na e-Uslugu, tj. ovlastiti ju da u ime opunomoćitelja može imati određena autorizacijska prava na e-uslugu.

Pružatelji elektroničke usluge trebaju ispuniti određene korake da bi se mogli integrirati s e-Ovlaštenjima. Formalni uvjeti definirani su u dokumentu „**Protokol rada e-Ovlaštenja**“, dok su tehnički preduvjeti definirani u nastavku.

Tehnička integracija poslužitelja e-usluge s e-Ovlaštenjima obavlja se na način da pružatelj e-usluge:

1. implementira e-uslugu na poslužitelj e-usluge u formi web aplikacije dostupne putem Interneta
2. pribavi poslužiteljski X509 certifikat (SSL certifikat) i njime zaštiti prethodno pripremljenu e-uslugu
3. pribavi Fina aplikacijski X509 certifikat za e-uslugu kojim će štiti komunikaciju s e-Ovlaštenja (ukoliko je napravljena integracija sa NIAS-om, koristi se certifikat koji se koristi i u komunikaciji sa NIAS-om)
4. preuzme javni ključ Fina aplikacijskog certifikata usluge e-Ovlaštenja
5. implementira formu u obliku web obrasca na kojoj će korisnik moći dati e-Punomoći na e-uslugu.
6. implementira prihvata XML poruke zahtjeva za ovlaštenjem (šalje e-Ovlaštenja) te slanje XML poruke odgovora (šalje e-usluga) sa podacima ovlaštenjima sa web obrasca za dodjelu prava korisnicima na e-Uslugu.
7. dostavi usluzi e-Ovlaštenja URL web stranice na kojoj e-usluga prihvaća poruku zahtjeva za web obrazac za dodjelu prava korisnicima na e-Uslugu, a koja omogućuje čitanje XML poruke zahtjeva od e-Ovlaštenja
8. dostavi usluzi e-Ovlaštenja aplikacijski certifikat kojime predmetna usluga štiti komunikaciju s e-Ovlaštenjima ali bez privatnog ključa, dakle, certifikat u .cer ili .p7b formatu.

Za implementaciju XML poruka koje pružatelj e-usluge izmjenjuje sa e-Ovlaštenjima može koristiti integracijske primjere koje nudi e-Ovlaštenja ili izraditi vlastite prema XSD shemama iz priloga *ePoslovanje_Sheme.zip*.

Poslužiteljski certifikati na strani e-usluge su obavezni jer se primjenom SSL protokola značajno podiže razina sigurnosti na relacijama:

Pružatelj e-usluge <-> e-Ovlaštenja

Korisnik <-> Pružatelj e-usluge.

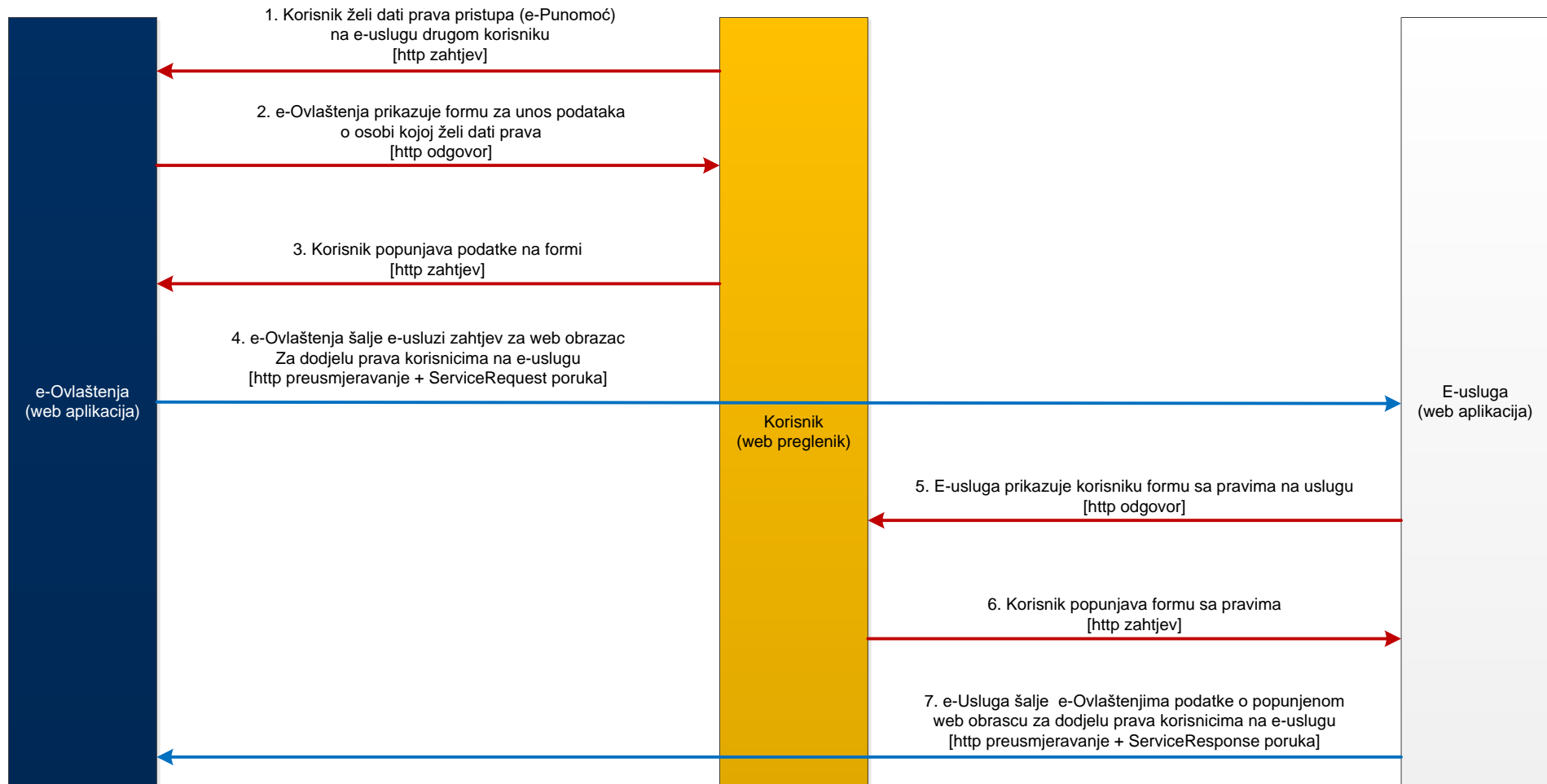
Središnji državni ured za razvoj digitalnog društva	Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja		
	Projekt: e-Poslovanje	Komponenta: e-Ovlaštenja	Djelokrug: FINA
	Datum: 19.02.2024.	Namjena: Za dionike u projektu	Verzija: 2.3

2.1 Dijagram tijeka komunikacije

Dijagram prikazan u nastavku prikazuje tijek komunikacije između korisnika: pružatelja elektroničke usluge i usluge e-Ovlaštenja.

Za integraciju elektroničke usluge s e-Ovlaštenjima nužno je da pružatelj e-usluge na poslužitelju e-usluge implementira dio koji omogućuje čitanje XML poruke dobivene od e-Ovlaštenja (korak 4. u dijagramu) te kreiranje XML poruke odgovora i slanje odgovora e-Ovlaštenjima (korak 7 u dijagramu).

Središnji državni ured za razvoj digitalnog društva	Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja		
	Projekt: e-Poslovanje	Komponenta: e-Ovlaštenja	Djelokrug: FINA
	Datum: 19.02.2024.	Namjena: Za dionike u projektu	Verzija: 2.3.



1. Dijagram tijeka komunikacije kod izrade web obrasca za dodjelu prava korisnicima na e-uslugu

Središnji državni ured za razvoj digitalnog društva	Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja		
	Projekt: e-Poslovanje	Komponenta: e-Ovlaštenja	Djelokrug: FINA
	Datum: 19.02.2024.	Namjena: Za dionike u projektu	Verzija: 2.3

Korak 1. Korisnik dolazi na e-Ovlaštenja i želi dati e-Punomoći drugoj osobi na određenu e-uslugu. [http zahtjev].

Korak 2. Usluga e-Ovlaštenja korisniku prikazuje formu za unos podataka o korisniku kojem se želi dati pravno pristupa na e-uslugu. [http odgovor]

Korak 3. Korisnik popunjava formu s podacima korisnika i potvrđuje unos podataka. [http zahtjev].

Korak 4. Usluga e-Ovlaštenja čita podatke s forme te generira ServiceRequest poruku zahtjeva unutar koje se nalaze podaci o osobi koja želi dati e-Punomoći na e-uslugu i osobi kojoj se daju e-Punomoći te ju šalje e-usluzi. [http preusmjeravanje + Service Request poruka]

Korak 5. E-usluga zaprimi zahtjev od e-Ovlaštenja, obradi ga te korisniku prikaže formu web obrasca za dodjelu prava korisnicima na e-uslugu na kojoj može odabrati koja prava na uslugu želi dati. [http odgovor]

Korak 6. Korisnik odabire koja prava na uslugu želi dati drugoj osobi te potvrđuje unos. U ovom koraku korisnik može odustati od davanja e-Punomoći na e-uslugu. [http zahtjev]

Korak 7. E-usluga zaprimi zahtjev podatke s forme koju je korisnik popunio, provjerava ih te kreira Service Request poruku i preusmjeri korisnika na uslugu e-Ovlaštenja. Poruka odgovora sadrži podatke o Pravima pristupa (u obliku ključ/vrijednost) na e-uslugu. [http preusmjeravanje + Service Response poruka]

Ukoliko je korisnik odustao od davanja e-Punomoći tada se korisnik samo preusmjeri na URL GET metodom koji je dobiven u poruci zahtjeva od e-Ovlaštenja. [http preusmjeravanje]

NAPOMENA: Nakon 7. koraka na e-Ovlaštenjima se kreira dokument ovlaštenja koji postaje aktivan nakon što ga digitalno potpišu sve osobe ovlaštene za zastupanje (ukoliko se radi o pravnoj osobi), te osoba koja je dobila pravo pristupa na uslugu.

2.2 Specifikacija protokola

Usluga e-Ovlaštenja se temelji na razmjeni poruka između tri različita entiteta: korisnika, pružatelja e-usluge i e-Ovlaštenja. Uloga korisnika je pasivna te on služi samo kao transportni sloj u razmjeni poruka, e-Ovlaštenja i e-usluga su aktivni (engl. endpoints) što znači da prilikom dobivanja zahtjeva moraju dati odgovor.

Razmjena poruka odvija se temeljem HTTP-POST redirect binding protokola.

2.2.1 HTTP Redirect Binding protokol

HTTP Redirect Binding protokol propisuje razmjenu poruka preko korisnika pomoću HTTP/HTTPS transportnog sloja. Poruke se razmjenjuju tako da se potpisuju na strani poslužitelja te se korisnik zajedno s porukom preusmjerava na server kojemu je ta poruka namijenjena. Iako je korisnik nosilac poruke, na ovaj je način razmjena poruka u potpunosti osigurana te su poruke nepromjenjive.

Središnji državni ured za razvoj digitalnog društva	Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja		
	Projekt: e-Poslovanje	Komponenta: e-Ovlaštenja	Djelokrug: FINA
	Datum: 19.02.2024.	Namjena: Za dionike u projektu	Verzija: 2.3

Protokol se dijeli na razmjenu poruka pomoću HTTP Redirect i HTTP POST metode. U slučaju e-Ovlaštenja koristit ćemo HTTP POST metodu za uspješan odgovor i HTTP GET za odustajanje i neuspješan odgovor.

2.2.2 HTTP POST metoda

HTTP-POST je oblik je HTTP-REDIRECT Binding protokola koji koristi POST metodu internetskog preglednika za slanje podataka. Ovdje je potrebno korisniku stvoriti HTML stranicu s HTML formom koja će podatke poslati na određeni poslužitelj. HTML forma treba imati sljedeće parametre (HTML input elemente):

- ServiceRequest (šalju e-Ovlaštenja kod preusmjerenja korisnika na e-uslugu)
- ResponseUrl (šalju e-Ovlaštenja)
- CancelUrl (šalju e-Ovlaštenja)
- ServiceResponse (šalje e-usluga e-Ovlaštenjima kod preusmjerenja korisnika na e-Ovlaštenja)

Formiranje HTTP POST forme izvodi se sa sljedećim koracima:

- Method parametar forme je potrebno postaviti na POST
- Action parametar forme je potrebno postaviti na određenu adresu
- Dodaje se sakriveni `<input name="ServiceRequest">` ili `<input name="ServiceResponse">` element koji sadrži Base64 enkodiranu ServiceRequest poruku / ServiceResponse poruku

HTML forma može sadržavati JavaScript koji radi automatsko slanje podataka (engl. submit), ali mora i sadržavati gumb s kojim korisnik može sam pokrenuti slanje podataka s HTML forme u slučaju da je JavaScript blokiran u internetskom pregledniku.

2.3 Specifikacija poruka

Komunikacija između pojedinih entiteta odvija se putem XML poruka. Kod davanja e-Punomoći na e-uslugu izmjenjuju se dva tipa XML poruka, a to su ServiceRequest i ServiceResponse poruke. Kompletni primjeri nalaze se u prilogu specifikacije *PrimjeriPoruka_RegistracijskiObrascac.zip*. Definicije modela elemenata potrebne za deserijalizaciju i serijalizaciju opisane su putem XSD datoteka u prilogu *ePoslovanje_sheme.zip*. Poruka ne smije sadržavati BOM zaglavlje.

2.3.1 ServiceRequest

Poruka za zahtjev za izradu autorizacijskog obrasca od strane e-usluge naziva se ServiceRequest poruka. Poruka sadrži sve podatke o osobi koja daje e-Punomoći i osobi koja prima prava, te e-usluga na osnovu ti podatka popunjava dio podataka na obrascu.

Pročišćeni primjer poruke je sljedeći:

Središnji državni ured za razvoj digitalnog društva	Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja		
	Projekt: e-Poslovanje	Komponenta: e-Ovlaštenja	Djelokrug: FINA
	Datum: 19.02.2024.	Namjena: Za dionike u projektu	Verzija: 2.3

```

<?xml version="1.0" encoding="utf-8"?>
<ServiceRequest xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" Id="_2ec0893bb5ef40ed850edd2959615674" ExpiryTime="2020-11-
05T07:47:15.2246079+01:00" xmlns="http://eovlastenja.fina.hr/authorizationdocument/v3">
  <AuthorizationInfo>
    <ServiceSubjectName>CN=Test Servis 2, L=ZAGREB, OID.2.5.4.97=HR85821130368, O=FINA, C=HR</ServiceSubje
ctName>
    <FromEntity>
      <Person>
        <LocalPerson xmlns="http://eovlastenja.fina.hr/authorizationbase/v2">
          <OIB>123</OIB>
          <FirstName>IVAN</FirstName>
          <LastName>HORVAT</LastName>
        </LocalPerson>
      </Person>
      <Legal>
        <Name xmlns="http://eovlastenja.fina.hr/authorizationbase/v2">FINANCIJSKA AGENCIJA</Name>
        <Jips xmlns="http://eovlastenja.fina.hr/authorizationbase/v2">
          <IPS>85821130368</IPS>
          <IZVOR_REG>1</IZVOR_REG>
        </Jips>
      </Legal>
    </FromEntity>
    <ForEntity>
      <Legal xmlns="http://eovlastenja.fina.hr/authorizationbase/v2">
        <Name>FINANCIJSKA AGENCIJA</Name>
        <Jips>
          <IPS>85821130368</IPS>
          <IZVOR_REG>1</IZVOR_REG>
        </Jips>
      </Legal>
    </ForEntity>
    <ToEntity>
      <CertificateDN />
      <Person>
        <OIB xmlns="http://eovlastenja.fina.hr/authorizationbase/v2">123</OIB>
        <FirstName xmlns="http://eovlastenja.fina.hr/authorizationbase/v2">IVAN</FirstName>
        <LastName xmlns="http://eovlastenja.fina.hr/authorizationbase/v2">HORVAT</LastName>
      </Person>
      <Legal>
        <Name xmlns="http://eovlastenja.fina.hr/authorizationbase/v2">FINANCIJSKA AGENCIJA</Name>
        <Jips xmlns="http://eovlastenja.fina.hr/authorizationbase/v2">
          <IPS>85821130368</IPS>
          <IZVOR_REG>1</IZVOR_REG>
        </Jips>
      </Legal>
    </ToEntity>
  </AuthorizationInfo>
</ServiceRequest>

```

Središnji državni ured za razvoj digitalnog društva	Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja		
	Projekt: e-Poslovanje	Komponenta: e-Ovlaštenja	Djelokrug: FINA
	Datum: 19.02.2024.	Namjena: Za dionike u projektu	Verzija: 2.3

```

    <Email />
  </ToEntity>
  <ValidFrom>2020-11-05T00:00:00+01:00</ValidFrom>
  <ActivePermissions>
    <Permission>
      <Key>ULOGA</Key>
      <Value>admin</Value>
      <Description>Razina pristupa</Description>
      <ValueDescription>Administrator</ValueDescription>
    </Permission>
    <Permission>
      <Key>PRAVO</Key>
      <Value>read</Value>
      <Description>Ovlasti</Description>
      <ValueDescription>Čitanje</ValueDescription>
    </Permission>
    <Permission>
      <Key>PDV</Key>
      <Value>True</Value>
      <Description>Pravo predaje PDV obrasca</Description>
      <ValueDescription>Da</ValueDescription>
    </Permission>
  </ActivePermissions>
</AuthorizationInfo>
<TemplateInfo>
  <LegalDocumentType>PRISTUP</LegalDocumentType>
  <IsDirect>true</IsDirect>
  <IsReferent>>false</IsReferent>
</TemplateInfo>
<Signatures>
  <Signature Id="RoRequestSignature" xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
      <Reference URI="#_2ec0893bb5ef40ed850edd2959615674">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <DigestValue>DcL1fKeeYmjvkdqafZOCOaAHyJo=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>...</SignatureValue>
  </KeyInfo>

```

Središnji državni ured za razvoj digitalnog društva	Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja		
	Projekt: e-Poslovanje	Komponenta: e-Ovlaštenja	Djelokrug: FINA
	Datum: 19.02.2024.	Namjena: Za dionike u projektu	Verzija: 2.3

```

<KeyName>CN=Upravljanje-
eOvlastenjimaTst, L=ZAGREB, OID.2.5.4.97=HR85821130368, O=FINA, C=HR</KeyName>
<KeyValue>
  <RSAKeyValue>
    <Modulus>...</Modulus>
    <Exponent>AQAB</Exponent>
  </RSAKeyValue>
</KeyValue>
<X509Data>
  <X509Certificate>...</X509Certificate>
</X509Data>
</KeyInfo>
</Signature>
</Signatures>
</ServiceRequest>

```

Elementi ServiceRequest poruke su sljedeći:

- ServiceRequest kao osnovni (engl. root) element
- AuthorizationInfo
- TemplateInfo
- Signatures

ServiceRequest element:

- *Id* atribut – GUID, jedinstveni identifikator poruke, svaka poruka mora posjedovati svoj jedinstveni identifikator.
- *ExpiryTime* atribut – vrijeme do kada poruka vrijedi

AuthorizationInfo element:

- *ServiceSubjectName element* – SubjectName aplikacijskog certifikata kojom se servis predstavlja e-Ovlaštenjima
- *FromEntity* element – sadrži podatke o fizičkoj i/ili pravnoj osobi koja daje u svoje ime ili u ime nekog drugog ovlaštenje
- *ForEntity* element – sadrži podatke o fizičkoj ili pravnoj osobi za koju se daje ovlaštenje
- *ToEntity* element – sadrži podatke o osobi / certifikatu kojoj se daje ovlaštenje
 - CertificateDN element – ukoliko se servis prihvaća ovlaštenja preko DN-a certifikata, tada je ovaj element popunjen
 - ApplicativeCertificateDN element – ukoliko se e-Punomoći daju na aplikativni certifikat, tada ovaj element mora biti popunjen

Središnji državni ured za razvoj digitalnog društva	Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja		
	Projekt: e-Poslovanje	Komponenta: e-Ovlaštenja	Djelokrug: FINA
	Datum: 19.02.2024.	Namjena: Za dionike u projektu	Verzija: 2.3

- *ValidFrom* element – vrijeme od kojega dokument počinje važiti
- *ActivePermissions* element – ukoliko osoba već posjeduje prava na e-uslugu, tada se ta postojeća prava šalju u *ServiceRequest* e-usluzi kako bi usluga mogla prikazati na obrascu koja prava na e-uslugu osoba već ima.

TemplateInfo element:

- *LegalDocumentType* element – određuje tip dokumenta ovisno o tome na koji način i tko daje e-Punomoći na uslugu. Isto tako određuje naziv obrasca e-usluge
 - PUNOMOC – Ovlast za zastupanje koju Opunomoćitelj daje Opunomoćeniku u Podsustavu e-Ovlaštenja (Naziv obrasca – Punomoć za pristup na e-uslugu).
 - PRISTUP – ovlast za pristup na e-uslugu koju Opunomoćitelj daje sam sebi (kao fizičkoj osobi koja djeluje u ime Poslovnog subjekta) ili daje nekoj drugoj fizičkoj osobi koja djeluje unutar istog Poslovnog subjekta kao Opunomoćeniku u Podsustavu e-Ovlaštenja (Naziv obrasca – Pristup na e-uslugu).
 - IZJAVA – Ovlast za zastupanje koju Opunomoćitelj daje sam sebi kao ovlaštenoj osobi za zastupanje po zakonu nekog drugog Poslovnog subjekta ili sebi kao Fizičkoj osobi – građaninu kao Opunomoćeniku u Podsustavu e-Ovlaštenja (Naziv obrasca – Izjava o suglasnosti za pristup na e-uslugu).¹
- *IsDirect* element – da li je osoba koja daje e-Punomoć djeluje samostalno ili preneseno (djeluje u tuđe ime)

IsReferent element- da li referent djeluje u ime osobe koja daje e-Punomoći (Referent je osoba na „šalteru“ koja proces davanja e-Punomoći može napraviti umjesto korisnika)

Signatures element sadrži:

- *Signature element*: - ovaj element definiran je XML-Sig standardom. Usluga e-Ovlaštenja potpisuje *ServiceRequest* poruke aplikacijskim certifikatom namijenjenim za komunikaciju s e-uslugama

Elementi Person i Legal

Ova dva elementa sadrže podatke o pravnoj/fizičkoj osobi

- Person
 - OIB – oib fizičke osobe

¹ TemplateInfo elementi određuju kakav se tip dokumenta kreira u bazi prema pravnom tumačenju. Konkretno, Izjava ne znači da ovlaštena osoba treba sam sebi dati ovlast za zastupanje nego ako Opunomoćitelj koji je ovlaštena osoba poslovnog subjekta za koji se daje ovlast za zastupanje daje sam sebi u nekom drugom poslovnom subjektu gdje je također ovlaštena osoba tu istu ovlast za zastupanje, pravno gledano formira se Izjava a ne Punomoć ili Pristup.

Središnji državni ured za razvoj digitalnog društva	Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja		
	Projekt: e-Poslovanje	Komponenta: e-Ovlaštenja	Djelokrug: FINA
	Datum: 19.02.2024.	Namjena: Za dionike u projektu	Verzija: 2.3

- FirstName – ime fizičke osobe
- LastName – prezime fizičke osobe
- Legal
 - Name – dugi naziv poslovnog subjekta
 - Jips² - Jedinstveni Identifikator Poslovnog subjekta koji se sastoji od dva odvojena kombinirana polja
 - IPS – Identifikator Poslovnog Subjekta
 - IZVOR_REG – Izvor kojem pripada Poslovni Subjekt

² Opisano detaljnije u protokolu rada NIAS-a za e-Građane i e-Poslovanje i u prilogu e-Poslovanje_sifarnik.xlsx

Središnji državni ured za razvoj digitalnog društva	Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja		
	Projekt: e-Poslovanje	Komponenta: e-Ovlaštenja	Djelokrug: FINA
	Datum: 19.02.2024.	Namjena: Za dionike u projektu	Verzija: 2.3

2.3.2 ServiceResponse

ServiceResponse (XML Response element) odgovor je na zahtjev za davanje e-Punomoći na odabranu e-uslugu. Uspješan odgovor se upućuje HTTP POST metodom na lokaciju dobivenu u samom zahtjevu dobiven pod argumentom *ResponseUrl*. Ukoliko korisnik odustane od kreiranja obrasca ili zahtjev ne zadovoljava interna poslovna tada se neuspješan odgovor upućuje HTTP GET metodom na lokaciju dobivenu u samom zahtjevu dobiven pod argumentom *CancelUrl*.

Primjer zahtjeva za odustajanje

- Odustajanje korisnika od davanja pristupnih prava na registracijskom obrascu korisnika se preusmjerava natrag na e-Ovlaštenja na način da se CancelUrl linku doda query parametar *requestId* koji označava Id zahtjeva koji je e-Ovlaštenja poslao e-usluzi. Dobivenim URL-om se preusmjerava korisnika HTTP GET metodom natrag.

Primjer URL-a za odustajanje od davanja ovlaštenja

https://eovlastenjatst.fina.hr/Home/CancelAuthorizeResponse?requestId=_4b28c56d03244ed5aba27ba95b68b2da

- Ukoliko se dogodi greška na strani obrasca prilikom generiranja obrasca CancelUrl-u se osim *requestId*-a, dodaje i *errorMsg* parametar, koji sadrži poruku o grešci koja će se prikazati korisniku na ekranu e-Ovlaštenja. Greška ne mora nužno biti tehničke naravi, mogu to biti interna poslovna ograničenja.

Primjer URL-a kada se dogodi greška na strani obrasca

https://eovlastenjatst.fina.hr/Home/CancelAuthorizeResponse?requestId=_4b28c56d03244ed5aba27ba95b68b2da&errorMsg=Dogodila%20se%20gre%C5%A1ka

Pročišćeni primjer ServiceResponse poruke:

```
<?xml version="1.0" encoding="utf-8"?>
<ServiceResponse xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Id="_ServiceResponse" ForRequestId="_2ec0893bb5ef40ed850edd2959615674" xmlns="http://eovlastenja.fina.hr/authorizationdocument/v3">
  <ServiceData>
    <AuthorizationData>
      <Permissions>
        <Permission>
          <Key>ULOGA</Key>
          <Value>admin</Value>
          <Description>Razina pristupa</Description>
          <ValueDescription>Administrator</ValueDescription>
        </Permission>
        <Permission>
          <Key>PRAVO</Key>
          <Value>read/write</Value>
```


Središnji državni ured za razvoj digitalnog društva	Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja		
	Projekt: e-Poslovanje	Komponenta: e-Ovlaštenja	Djelokrug: FINA
	Datum: 19.02.2024.	Namjena: Za dionike u projektu	Verzija: 2.3

```

        <Description>Ovlasti</Description>
        <ValueDescription>Čitanje/Pisanje</ValueDescription>
    </Permission>
    <Permission>
        <Key>PDV</Key>
        <Value>True</Value>
        <Description>Pravo predaje PDV obrasca</Description>
        <ValueDescription>Da</ValueDescription>
    </Permission>
</Permissions>
</AuthorizationData>
</ServiceData>
<Signatures>
    <Signature Id="ServiceResponseSignature" xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
            <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
            <Reference URI="#_ServiceResponse">
                <Transforms>
                    <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                    <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </Transforms>
                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                <DigestValue>V9PtZK0L60V00og4k3MH1Cn9DzI=</DigestValue>
            </Reference>
        </SignedInfo>
        <SignatureValue>...</SignatureValue>
    <KeyInfo>
        <KeyName>CN=Test Servis 2, L=ZAGREB, OID.2.5.4.97=HR85821130368, O=FINA, C=HR</KeyName>
        <KeyValue>
            <RSAKeyValue>
                <Modulus>...</Modulus>
                <Exponent>AQAB</Exponent>
            </RSAKeyValue>
        </KeyValue>
        <X509Data>
            <X509Certificate>...</X509Certificate>
        </X509Data>
    </KeyInfo>
    </Signature>
</Signatures>
</ServiceResponse>

```

Elementi **ServiceResponse** poruke su sljedeći:

- ServiceResponse kao osnovni (engl. root) element XML poruke

Središnji državni ured za razvoj digitalnog društva	Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja		
	Projekt: e-Poslovanje	Komponenta: e-Ovlaštenja	Djelokrug: FINA
	Datum: 19.02.2024.	Namjena: Za dionike u projektu	Verzija: 2.3

- ServiceData
- AuthorizationData
- Signatures

ServiceResponse element:

- *Id* – oznaka poruke odgovora – uvijek ima vrijednost „_ServiceResponse“
- *ForRequestId* – Vrijednost Id iz ServiceRequest poruke, označuje za koji zahtjev se šalje odgovor

ServiceData element:

- kontejner elemenata AuthorizationData

AuthorizationData element:

- Permissions element je kontejner za listom Permission elemenata
- Permission element sadrži podatke o pravima pristupa (key/value)
 - Key element: sadrži ključ određenog prava, maksimalno 250 znakova
 - Value element: vrijednost prava, može biti i json, maksimalno 2000 znakova
 - Description element: opis prava za vizualnu reprezentaciju Key elementa, maksimalno 250 znakova, obavezan
 - ValueDescription element: opis prava za vizualnu reprezentaciju vrijednosti Value elementa, maksimalno 1000 znakova, obavezan

Signatures element sadrži:

- *Signature element*: - ovaj element definiran je XML-Sig standardom. Usluga e-Ovlaštenja zahtijeva da je XML poruka potpisana aplikacijskim certifikatom unaprijed definiranim prilikom integracije

Središnji državni ured za razvoj digitalnog društva	Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja		
	Projekt: e-Poslovanje	Komponenta: e-Ovlaštenja	Djelokrug: FINA
	Datum: 19.02.2024.	Namjena: Za dionike u projektu	Verzija: 2.3

2.4 Specifičnosti za pružatelje e-usluga

Uloga je pružatelja e-usluge pružanje usluge korisnicima elektroničkim putem. Komunikacija s pružateljem e-usluge uvijek se odvija u istom smjeru. Zahtjev za pravima pristupa ide od e-Ovlaštenja prema e-usluzi, a odgovor od e-usluge prema e-Ovlaštenjima.

Pružatelj e-usluge mora implementirati logiku da omogući prihvata XML poruke (Service Request) od usluge e-Ovlaštenja i prikaže korisniku HTML formu u obliku obrasca na kojem se nalaze pristupna prava za e-Uslugu.

Nakon što korisnik popuni podatke na registracijskoj formi i potvrdi formu, e-usluga mora kreirati XML poruku odgovora (ServiceResponse) u kojoj se nalaze svi podaci sa pristupnim pravima sa forme, HTML popunjenog obrasca (kako bi se mogla generirati slika u e-Ovlaštenjima).

Isto tako korisnik u trenutku stvaranja obrasca može odustati od davanja e-Punomoći, te se u tom trenutku radi preusmjerenje korisnika na određeni URL (dobiven u ServiceRequest poruci) natrag na e-Ovlaštenja.

Usluga e-Ovlaštenja razlikuje e-usluge po dva osnovna tipa, a to su:

- Način davanja e-Punomoći:
 - Po identifikatorima fizičke i pravne osobe
 - Po Dn-u certifikata na koji se daje e-Punomoć
- Tipu osoba za koje je usluga namijenjena:
 - Fizičke osobe
 - Pravne osobe
 - Fizičke i pravne osobe

NAPOMENA:

Usluga e-Ovlaštenja ni na koji način ne regulira registraciju fizičkih ili pravnih osoba unutar e-usluge. Što znači da ukoliko osoba želi dati e-Punomoći na poslovni subjekt koji nije registriran na e-usluzi, e-Ovlaštenja ju neće spriječiti.

Registraciju osoba, mora regulirati sama usluga preko registracijskog obrasca prije nego što korisniku prikaže web obrazac za dodjelu prava korisnicima na e-uslugu.

Središnji državni ured za razvoj digitalnog društva	Tehnička specifikacija za integraciju web registracijskog obrasca za dodjelu prava korisnicima na e-Uslugu u e-Ovlaštenja		
	Projekt: e-Poslovanje	Komponenta: e-Ovlaštenja	Djelokrug: FINA
	Datum: 19.02.2024.	Namjena: Za dionike u projektu	Verzija: 2.3

2.5 Sigurnost

Protokol kojim se provodi izdavanje i prijenos poruka u sustavu NIAS osiguran je standardnim algoritmima potpisivanja – RSA / DSA / SHA2. Kako bi se ispravno provjerila sigurnost poruka potrebno je implementirati sljedeći algoritam provjere za ServiceRequest i ServiceResponse poruke:

- provjeriti ispravnost XML-Sig potpisa kod HTTP-POST protokola; provjeriti je li certifikat kojim je XML poruka potpisana ispravan i je li potpisan od strane e-Ovlaštenja;
- sve poruke šalje se https kanalom (HTTPS protokol podrazumijeva kriptiranje mrežnog prometa između dvije krajnje točke pomoću serverskog TLS certifikata. Tako je nemoguće pročitati dio koji se odnosi na korisničku sjednicu.)
- provjeriti vrijeme valjanosti poruke i svih dijelova unutar nje;