Projekt e-Građani

Nacionalni identifikacijski i autentifikacijski sustav (NIAS)

Tehnička specifikacija za „Single Sign-Out" e-usluga

Verzija 1.0

Sadržaj

Povijest promjena

Br.	Verzija	Opis	Datum	Autori
1.	0.1	Radna verzija – draft	18.11.2013.	Fina
2.	1.0	Objedinjena poglavlja 2. i 3.; unificiran format dokumenta; promijenjena oznake verzije iz 'Radna' u 'Službena'; odobrena objava	20.11.2013.	Ministarstvo uprave

1. Uvod

Ovaj dokument ima svrhu definiranja tehničkih preduvjeta koje je nužno ispuniti da bi se ostvarila integracija pružatelja e-usluga s NIAS-om te ima svrhu specificiranja načina razmjene podataka između pružatelja e-usluga i NIAS-a, a sve u cilju sigurne razmjene podatka nužnih za proces jedinstvene odjave korisnika. Način razmjene podatka između NIAS-a i pružatelja e-usluga izveden je iz dosadašnjih najboljih praksi, koje osiguravaju sigurnu isporuku i zadovoljavanje visoke razine sigurnosti, odnosno zaštite prijenosa i kontrole nepovredivosti sadržaja.

Koncept Sustava NIAS objašnjen je u dokumentu „Protokol rada NAIS-a" na kojeg se ova specifikacija direktno veže.

2. Preduvjeti za integraciju pružatelja e-usluga

NIAS ima ulogu posrednika između krajnjeg korisnika – vlasnika vjerodajnice, pružatelja elektroničke usluge i izdavatelja vjerodajnice. Njegova je osnovna svrha da pružateljima e-usluga olakša identifikaciju korisnika koji posjeduju različite vjerodajnice izdane od ovlaštenih izdavatelja vjerodajnica te da korisnicima omogući uporabu različitih vjerodajnica na različitim e-uslugama ovisno o razni sigurnosti koju te e-usluge zahtijevaju. Pri tome, NIAS umjesto e-usluge šalje upit izdavatelju vjerodajnice kako bi se provjerila njezina autentičnost. Nakon uspješne provjere, pružatelju e-usluge dostavlja identifikacijske podatke o korisniku na temelju kojih e-usluga odobrava pristup korisniku.

Pružatelji elektroničke usluge trebaju ispuniti određene korake da bi se mogli integrirati s NIAS-om. Formalni uvjeti definirani su u dokumentu „Protokol rada NIAS-a", dok su tehnički preduvjeti definirani ovdje.

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

1. implementira e-uslugu na poslužitelj e-usluge u formi web aplikacije dostupne putem Interneta
2. implementira mehanizam čuvanja i mapiranja SessionIndex te NameId elementa AuthnResponse poruke sa vlastitim mehanizmom za sigurne sjednice
3. pribavi Fina aplikacijski X509 certifikat za e-uslugu kojim će štititi komunikaciju s NIAS-om
4. preuzme NIAS-ov Fina aplikacijski certifikat sa javnim ključem kojim NIAS štiti komunikaciju
5. implementira SAML protokol za SSO (single sign out) kojim se ostvaruje komunikacija između e-usluge i NIAS-a te NIAS-a i e-usluge korištenjem pribavljenog X509 aplikacijskog certifikata i porukama prema specifikaciji u nastavku
6. dostavi NIAS-u URL web stranice na kojoj e-usluga očekuje zahtjev ili odgovor od NIAS-a, a koja implementira SAML protokol i omogućuje zaprimanje i obradu LogoutRequest ili LogoutResponse poruke od NIAS-a. E-usluga treba implementirati dva protokola (HTTP i SOAP) te smije imati različite web stranice za pojedini protokol jednostruke odjave.
7. dostavi NIAS-u aplikacijski certifikat kojime e-usluga štiti komunikaciju s NIAS-om ali bez privatnog ključa, dakle, u .cer ili .p7b formatu
8. dostavi NIAS-u SSL certifikat kojim će e-usluga štititi SOAP kanal komunikacije, ali bez privatnog ključa, dakle u .cer ili .p7b formatu

Za implementaciju SAML protokola pružatelj e-usluge može koristiti integracijske biblioteke koje nudi NIAS, integracijske biblioteke od trećih strana ili izraditi vlastite biblioteke koje podržavaju SAML standard i sadrže logiku kojom se ostvaruje veza između dva sustava.

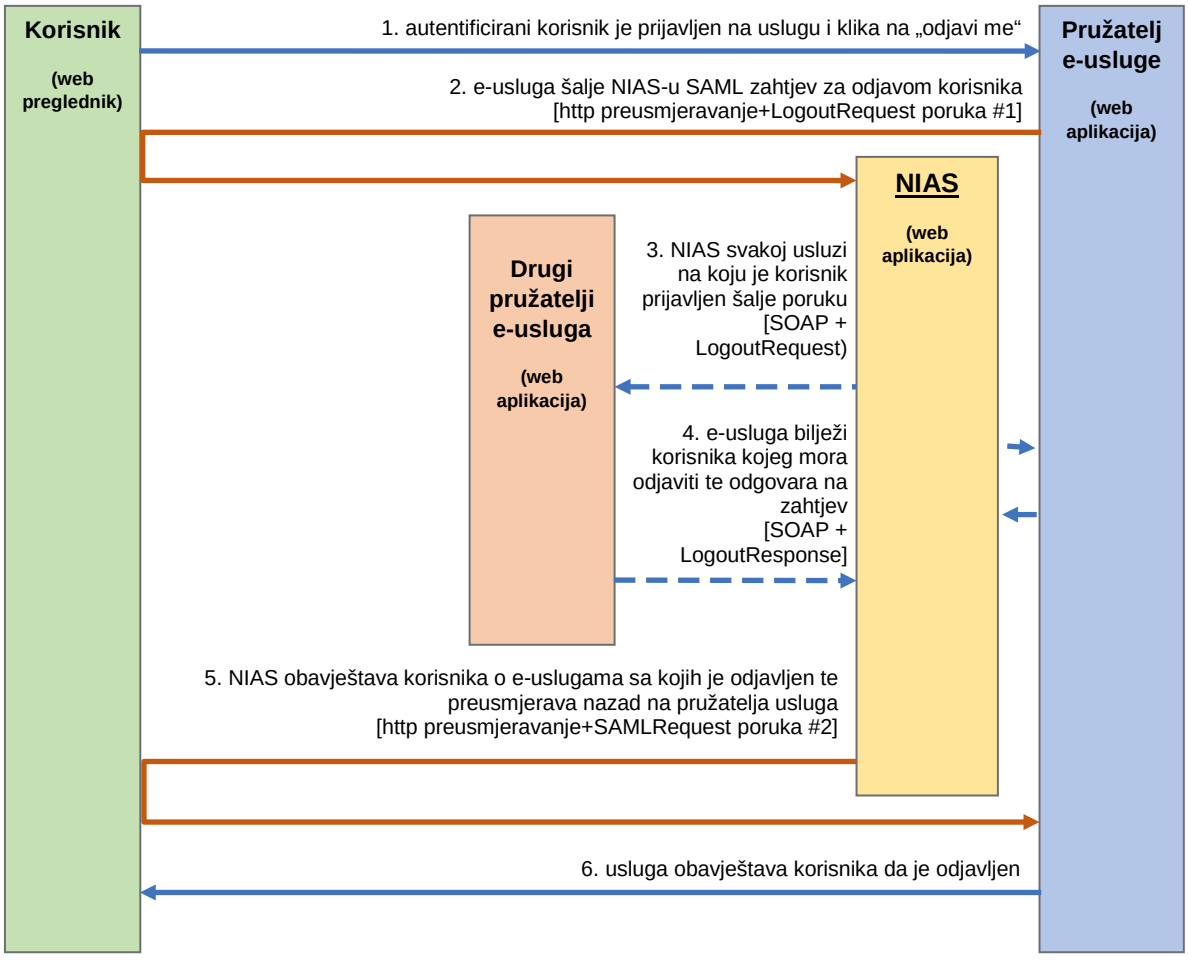
Pružatelju e-usluge se preporučuje da pribavi Fina poslužiteljski X509 certifikat za zaštitu komunikacije između korisnika i poslužitelja e-usluge (SSL certifikat) i njime zaštiti prethodno pripremljenu e-uslugu.

3. Tehnička specifikacija za Single Sign-Out

3.1 Dijagram tijeka komunikacije

Dijagram prikazan u nastavku prikazuje tijek komunikacije između korisnika: poslužitelja elektroničke usluge, NIAS-a i te ostalih poslužitelja elektroničkih usluga koje se nalaze u istoj sjednici.

Za integraciju jedinstvene odjave elektroničke usluge sa NIAS-om nužno je da pružatelj e-usluge na poslužitelju e-usluge implementira dio SAML protokola koji omogućuje slanje i zaprimanje SAML zahtjeva za odjavom (LogoutRequest) te zaprimanje i slanje SAML odgovora za odjavom (LogoutResponse) i njegovu obradu.



Korak 1. Autentificirani korisnik je prijavljen na e-uslugu te se želi odjaviti. E-usluga na kojoj se korisnik trenutno nalazi je implementirala protokol jedinstvene odjave korisnika [http zahtjev].

Korak 2. Elektronička usluga zaprimi zahtjev, provjeri identitet korisnika te, nakon što ustanovi da je korisnik autentificiran, generira SAML zahtjev za odjavom (LogoutRequest poruka #2) i preusmjerava korisnika na NIAS. SAML zahtjev za odjavom, među ostalim, sadrži vremenski interval valjanosti zahtjeva, razlog odjave, ID korisnika koji se odjavljuje i certifikat za digitalno potpisivanje. Slanje zahtjeva na NIAS obavlja se putem korisnika na način da se korisnikov web preglednik preusmjeri na NIAS noseći pritom LogoutRequest poruku [http preusmjeravanje + LogoutRequest poruka #2].

Korak 3. NIAS zaprima zahtjev za odjavom, provjerava njegovu valjanosti i nakon obrade zahtjeva kontaktira svaku e-uslugu koja sudjeluje u korisničkoj sjednici. Svakoj usluzi se pomoću SOAP protokola šalje SAML zahtjev za odjavom korisnika. [SOAP + LogoutRequest]

Korak 4. Pojedina usluga odjavljuje korisnika te odgovara na zahtjev sa SAML odgovorom LogoutResponse [SOAP + LogoutResponse].

Korak 5. Kada NIAS zaprimi odgovore (ili greške) od svih e-usluga koje su sudjelovale u trenutnoj korisničkoj sjednici, korisnik se izvještava o svim odjavama te uspješnosti njih. Nakon 10 sekundi ili klikom na link korisnik se preusmjerava nazad na e-uslugu na kojoj je korisnik zatražio odjavu. [http odgovor – http preusmjeravanje].

Korak 6. E-usluga zaprima SAML odgovor LogoutResponse te odjavljuje korisnika i prikazuje odgovarajuću poruku kako se korisnik uspješno odjavio. [http odgovor].

Napomena: e-usluga koja je zatražila LogoutRequest će biti kontaktirana zajedno sa svim ostalim e-uslugama na kojima korisnik posjeduje sjednicu tijekom koraka 3, stoga se preporuča da e-usluga odjavljuje korisnika tek prilikom koraka 3 odnosno prilikom primanja LogoutRequest poruke od NIAS-a temeljem SOAPoverHTTP protokola.

3.2 Specifikacija protokola

Single Sign-Out (SSO) se temelji na razmjeni poruka između dva različita entiteta: pružatelja e-usluge i NIAS-a. Uloga korisnika je pasivna te on služi samo kao transportni sloj u razmjeni poruka, ostali entiteti su aktivni (engl. endpoints) što znači da prilikom dobivanja zahtijeva moraju dati odgovor. Razmjena poruka odvija se temeljem izdvojenih protokola koje definira SAML 2.0 standard, a za potrebe SSO su odabrana tri protokola – HTTP-GET i HTTP-POST redirect binding (indirektno) te SOAP over HTTP binding (direktno).

3.2.1 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 nosioc poruke o svojoj autentifikaciji, potpisom je poruka u potpunosti osigurana od nepromjenjenjivosti.

Ovaj protokol se dijeli na razmjenu poruka pomoću HTTP GET i HTTP POST metode.

3.2.2 HTTP GET metoda

HTTP GET metoda podrazumijeva slanje svih parametara SAML poruke pomoću URL-a. Poruka se može direktno predati na način da se korisniku na stranici generira poveznica (engl. hyperlink) sa URL-om koja korisnika zajedno sa SAML porukom vodi na određeni poslužitelj.

Poveznica mora sadržavati URL sa četiri parametra:

1. LogoutRequest / LogoutResponse (u ovisnosti o tome koja poruka se šalje) – SAML poruka koja je opisana kasnije u poglavlju LogoutRequest ili LogoutResponse.
2. RelayState – parametar koji sadrži specifični identifikator pošiljatelja (prilikom SAML odgovora ovo polje mora biti jednako vrijednosti koje je poslano SAML zahtjevom). Ovaj je identifikator u potpunosti nevezan za SAML protokol te se koristi samo za potrebe asinkronog mehanizma obrade podataka na serveru koji zadaje zahtjev.
3. SigAlg – URI koji je definiran XML-Sig standardom koji opisuje algoritam potpisivanja koji je korišten prilikom XML potpisa SAML poruke. Dopuštene vrijednosti su:

   DSAwithSHA1 i

   RSAwithSHA1.
4. Signature – vrijednost potpisa

Formiranje HTTP GET URL-a izvodi se temeljem sljedećih koraka:

- Iz SAML poruke se odstranjuje <ds:Signature> element koji tu poruku potpisuje kako bi poruka bila manja;
- SAML poruka se sažima (komprimira) DEFLATE algoritmom [RFC1951];
- Sažeta (komprimirana) poruka se kodira base64 algoritmom [RFC2045];
- Base64 poruka se URL kodira te se sprema u GET parametar SAMLRequest ili SAMLResponse u ovisnosti o tipu poruke;
- Dodaje se RelayState parametar te se URL kodira;
- U slučaju da je SAML poruka bila potpisana potrebno je dodati potpis GET parametara. Potpis GET parametara se vrši slaganjem prethodno definiranih parametara u sljedeći format:

  SAMLRequest=value&RelayState=value&SigAlg=value

  Dobiveni znakovni niz potpisuje se pomoću algoritma definiranog SigAlg poljem, potom se Base64 kodira, prilagođuje URL formatu te na kraju dodaje kao Signature parametar GET metodi. Rezultirajući URL mora izgledati na sljedeći način:

  https://nias.eid.com.hr/authenticate.aspx?SAMLRequest=value&RelayState=value&SigAlg=value&Signature=value

3.2.3 HTTP POST metoda

HTTP-POST je drugi oblik 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 odredišni poslužitelj. HTML forma treba imati sljedeće parametre (HTML input elemente):

- LogoutRequest / LogoutResponse (u ovisnosti o poruci koja se šalje)
- RelayState

Formiranje HTTP POST forme izvodi se sa sljedećim koracima:

- Method parametar forme je potrebno postaviti na POST;
- Action parametar forme je potrebno postaviti na odredišnu adresu;
- Dodaje se skriveni <input name="SAMLRequest"> ili <input name="SAMLResponse"> element koji sadrži Base64 enkodiranu LogoutRequest / LogoutResponse poruku;
- Dodaje se sakriveni <input name="RelayState"> koji sadrži vrijednost poslanu LogoutRequest porukom ili proizvoljnu vrijednosti generiranu od strane koja šalje LogoutRequest 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.

3.2.4 SOAP over HTTP metoda

SOAP over HTTP metoda se temelji na slanju SOAP poruke putem HTTP protokola. Ona služi za direktnu komunikaciju između dva servera bez posredstva korisnika. U slučaju modula jedinstvene odjave to je komunikacija između e-usluge i NIAS-a. Tom metodom je podržan zahtjev jedinstvene odjave korisnika u slučaju detekcije nedopuštenih radnji, jer korisnik ne može blokirati proces jedinstvene odjave.

Slanje zahtjeva započinje tako da se formira potrebna SAML poruka sa svim pravilima potpisivanja ili enkripcije definiranim za nju. Nakon toga se stvara SOAP poruka sa SAML porukom u svom tijelu. SOAP poruka je čisti omot oko SAML-a te ne sadrži posebna zaglavlja. Tako stvorena poruka se HTTP-POST protokolom prenosi prema poslužitelju. Prilikom slanja poruke, obavezno je postaviti HTTP zaglavlje SOAPAction sa vrijednosti http://www.oasis-open.org/comittees/security.

Primjer poruke složenog zahtjeva za jedinstvenu odjavu korisnika:

```
POST /SamlService HTTP/1.1
Host: www.example.com
Content-Type: text/xml
Content-Length: nnn
SOAPAction: http://www.oasis-open.org/committees/security
<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
    <samlp:LogoutRequest>
      ...
    </samlp:LogoutRequest>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Primjer poruke složenog odgovora:

```
HTTP/1.1 200 OK
Content-Type: text/xml
Content-Length: nnnn
<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
    <samlp:LogoutResponse>
      ...
    </samlp:LogoutResponse>
    </SOAP-Env:Body>
```

3.3 Specifikacija poruka

Komunikacija između pojedinih entiteta u SAML-u odvija se putem poruka. U sklopu NIAS-a integrirano je 6 parova poruka (zahtjeva i odgovora) – poruke između NIAS-a i poslužitelja e-usluge za potrebe jedinstvene prijave korisnika na e-uslugu (engl. Single Sign-On), poruke između NIAS-a i autentifikacijskog poslužitelja za potrebe autentifikacije korisnika te poruke između NIAS-a i poslužitelja e-usluge za potrebe jedinstvene odjave korisnika (engl. Single Sign-Out).

3.3.1 LogoutRequest

Poruka za zahtjev za autentifikacijom korisnika od drugog poslužitelja naziva se AuthnRequest poruka. Ona je dio SAML standarda te propisuje uvjete i načine autentifikacije koje autentifikacijski server mora napraviti kako bi uspješno autentificirao korisnika za pojedinu uslugu. NIAS koristi izdvojeni set SAML standarda za AuthnRequest poruku. Primjer poruke je sljedeći:

```
<?xml version="1.0" encoding="utf-8"?>
<LogoutRequest xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xmlns:xsd="http://www.w3.org/2001/XMLSchema"
               ID="1f881bcd-60db-488f-bffe-6114c396d690"
               Version="2.0"
               IssueInstant="2013-09-11T09:21:21.016Z"
               Destination="destination"
               Reason="urn:oasis:names:tc:SAML:2.0:logout:user"
               NotOnOrAfter="2013-09-11T09:26:21.016Z"
               xmlns="urn:oasis:names:tc:SAML:2.0:protocol">
  <Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"
          xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
            CN=NIAS, OU=FINA 00332852, OU=Poslovni, OU=DEMO, O=FINA, C=HR
  </Issuer>
  <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
          xmlns="urn:oasis:names:tc:SAML:2.0:assertion">TID123456789</NameID>
  <SessionIndex>sessionIndex</SessionIndex>
</LogoutRequest>
```

Elementi LogoutRequest poruke su sljedeći:

- LogoutRequest kao osnovni (engl. root) element;
- Issuer;
- Signature;
- NameID;
- SessionIndex.

LogoutRequest element:

- *ID* atribut – GUID, jedinstveni identifikator poruke, svaka poruka mora posjedovat svoj jedinstveni identifikator.
- *Version* atribut – oznaka verzije SAML standarda koji se koristi – 2.0.
- *IssueInstant* atribut – trenutak izdavanja SAML poruke izražen UTC vremenskom oznakom.
- *Destination* atribut – odredišna adresa prema kojoj se SAML poruka šalje.
- *NotOnOrAfter* atribut – vrijeme nakon kojega SAML poruka ne vrijedi.
- *Reason* atribut – URI vrijednosta koja opisuje razlog odjave:
    - urn:oasis:names:tc:SAML:2.0:logout:user
        - Korisnik je zatražio odjavu
    - urn:oasis:names:tc:SAML:2.0:logout:admin
        - Administrator sustava je zatražio odjavu korisnika
    - urn:oasis:names:tc:SAML:2.0:logout:intrusion
        - Detektiran je pokušaj nedopuštenog korištenja NIAS-a

Issuer element:

- *Format* atribut – format zapisa o izdavatelju. NIAS dopušta samo sljedeći format:
    - urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName.
- *Vrijednost elementa* – SubjectName aplikacijskog certifikata kojim se servis predstavlja NIAS-u.

Signature element:

- *Vrijednost elementa*: - ovaj element definiran je XML-Sig standardom. NIAS zahtijeva da je SAML poruka potpisana aplikacijskim certifikatom namijenjenim za komunikaciju s NIAS-om.

NameID element:

- *Format* atribut – format indikatora kojim je prikazan identifikator korisnika, NIAS podržava tri identifikatora, usluga šalje indetifikator sa kojim je korisnik autentificiran usluzi:
    - urn:oasis:names:tc:SAML:2.0:nameid-format:entity - korisnik je usluzi predstavljen jedinstvenim identifikatorom koji nepromjenjiv, dvije različite usluge će imat isti identifikator za istu osobu
- Vrijednost elementa: identifikator osobe (prema odabranom formatu) koje se želi odjaviti.

SessionIndex element:

- Vrijednost elementa: indeks korisničke sjednice koju je potrebno ugasiti. Ovaj broj se dobiva prilikom dobivanja odgovora na AuthnRequest zahtjev. SessionIndex vrijednost osigurava postojanje više sjednica za pojedinog korisnika.

3.3.2 LogoutResponse

LogoutResponse (XML Response element) odgovor je na određeni zahtjev za odjavu korisnika. Poveznica sa zahtjevom na koji je odgovor vezan se nalazi u polju InResponseTo. Kada entitet primi autentifikacijski odgovor na njemu je potrebno provjeriti sigurnosne elemente popisane u poglavlju Sigurnost te nakon toga provjeriti je li status poruke jednak Success. Tek nakon tih radnji korisnik se smatra uspješno autentificiranim te se može prijeći na čitanje atributa o korisniku tj. identifikaciju korisnika u vlastitom sustavu.

Primjer odgovora na autentifikacijski zahtjev:

```
<?xml version="1.0" encoding="utf-8"?>
<LogoutResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                ID="d3c40d2f-94d8-469c-b3d7-be6b4fa1daa9"
                InResponseTo="1f881bcd-60db-488f-bffe-6114c396d690"
                Version="2.0"
                IssueInstant="2013-09-11T09:21:21.019Z"
                Destination="destination"
                xmlns="urn:oasis:names:tc:SAML:2.0:protocol">
  <Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"
          xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
      CN=NIAS, OU=FINA 00332852, OU=Poslovni, OU=DEMO, O=FINA, C=HR
  </Issuer>
  <Status>
    <StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </Status>
</LogoutResponse>
```

Elementi LogoutResponse poruke su sljedeći:

- LogoutResponse kao osnovni (engl. root) element XML poruke;
- Issuer;
- Signature;
- Status.

LogoutResponse element:

- ID – jedinstveni identifikator poruke.
- InResponseTo – identifikator zahtjeva povezanog sa odgovorom.
- Version – verzija SAML standarda – 2.0.
- IssueInstant – vrijeme izdavanja odgovora.
- Destination – adresa poslužitelja kojemu je odgovor namijenjen.

Issuer element:

- oznaka naziva aplikacijskog certifikata kojemu je poruka izdana.

Signature element:

- XML-Sig potpis poruke.

Status element, sadrži status odgovora:

- StatusCode:
  - urn:oasis:names:tc:SAML:2.0:status:Success - označava uspješnu autentifikaciju;
  - ostalo – u slučaju greške.
- StatusMessage - neobavezni element sa detaljnom porukom o trenutnom statusu.

4. Specifičnosti za pružatelje e-usluga

Svaka e-usluga mora implementirati barem dva protokola. Prvi protokol mora biti odabran tako da podržava slanje poruke preko korisnika (HTTP-POST ili HTTP-REDIRECT metoda), dok drugi protokol mora biti SOAPoverHTTP jer on podržava direktnu komunikaciju između dva poslužitelja. Obje metode mogu završavati na istoj URL adresi.

U akciji jednostruke odjave e-usluga može sudjelovati na dva načina:

1. ***e-usluga je pokretač jednostruke odjave***

   Ovaj scenarij počinje tako da korisnik prilikom korištenja e-usluge klikne na gumb „Odjavi me" na stranicama e-usluge. Izvršavanjem zahtjeva e-usluga mora stvoriti LogoutRequest poruku koju mora poslati na NIAS. Prilikom stvaranja LogoutRequest poruke važno je obratiti pozornost na ova dva polja:

   - **SessionIndex**
     - ovaj broj se nalazi u AuthnResponse poruci kojom se korisnik autentificirao prema e-usluzi;
     - broj služi za identificiranje pojedine sjednice korisnika (korisnik može odjednom imati više sjednica na različitim uređajima).
   - **NameId**
     - vrijednost ovog elementa te atribut **Format** ispunjavaju se također prema podacima dobivenima u AuthnResponse poruci kojom se korisnik autentificirao prema e-usluzi;
     - element služi kako bi se korisnik jednoznačno odredio na NIAS-u.

2. ***NIAS je pokretač jednostruke odjave***

   Drugi način jednostruke odjave je kada NIAS kontaktira pojedinu uslugu sa zahtjevom za jednostruku odjavu. Prilikom slanja zahtjeva za odjavom odabrana je metoda SOAP putem HTTP protokola zbog prednosti direktnog kontaktiranja servera. Prednost direktnog kontakta je u mogućnosti da se poruke šalju bez posredstva korisnika te je stoga dolazak poruke na odredište zagarantiran i neometan u slučaju nedopuštenih radnji.

   Scenarij počinje tako da korisnik na NIAS-u klikne gumb „Odjavi me" ili da NIAS dobije od neke usluge zahtjev za jednostrukom odjavom. Nakon toga NIAS šalje poruku LogoutRequest prema e-usluzi. E-usluga ima zadaću zapamtiti ID korisnika (prema odabranom NameID – format atributu) i SessionIndex koji je povezan sa tom korisničkom sjednicom (SessionIndex se dobiva prilikom autentifikacije korisnika te se nalazi u Response poruci NIAS-a prilikom autentifikacije). Nakon primitka poruke e-usluga putem istog protokola mora prema NIAS-u poslati LogoutResponse odgovor sa statusom *success* u slučaju uspješnog izvođenja radnje.

Prilikom prvog dolaska korisnika na e-uslugu, usluga mora prepoznati da je za korisnika izdan LogoutRequest te ga uspješno odjaviti odnosno ne dopustiti daljni rad putem iste sjednice. Prilikom prepoznavanja korisnika potrebno je obratiti pozornost na SessionIndex sjednice koju je potrebno odjaviti (primjer - ako se korisnik prijavio mobitelom i računalom, a samo na mobitelu stisnuo odjavi me).

5. Sigurnost

Protokol kojim se provodi izdavanje i prijenos poruka u sustavu NIAS osiguran je standardnim algoritmima potpisivanja – RSA / DSA / SHA1. Kako bi se ispravno provjerila sigurnost poruka potrebno je implementirati sljedeći algoritam provjere za LogoutRequest i LogoutResponse poruke:

- provjeriti ispravnost XML-Sig potpisa kod HTTP-POST protokola ili potpisa izvedenog iz Signature polja kod HTTP-GET protokola;
- provjeriti je li certifikat kojim je SAML poruka potpisana ispravan i je li potpisan od strane NIAS-a;
- provjeriti vrijeme valjanosti poruke i svih dijelova unutar nje;
- provjeriti je li se ID te poruke već prije koristio;
- provjeriti Destination polje i njegovo poklapanje s uslugom koja je dobila SAML poruku;
- provjeriti je li poruka odgovor na zahtjev koji je usluga prethodno poslala (InResponseTo element);
- provjeriti je li element Status poruke jednak Success te ako nije tada korisniku prikazati na ekranu StatusMessage poruku koja slijedi StatusCode.