Naziv projekta: e-Poslovanje

UP.04.1.1.16.0001

PARTNER

Financijska agencija

PROJEKTNA DOKUMENTACIJA

„Tehnička specifikacija za integraciju e-usluga u NIAS“

Datum:

lipanj, 2020.

Projekt je sufinancirala Europska Unija iz Europskog socijalnog fonda.
Sadržaj dokumenta isključiva je odgovornost Ministarstva uprave.

Projekt e-Poslovanje

Tehnička specifikacija za integraciju e-usluga u NIAS

Sadržaj

1. Uvod

Ovaj dokument ima svrhu definiranja tehničkih preduvjeta koje je nužno ispuniti da bi se ostvarila integracija pružatelja e-usluga s Nacionalnim identifikacijskim i autentifikacijskim sustavom (NIAS) te ima svrhu specificiranja načina razmjene podataka između pružatelja e-usluga i NIAS-a, a sve u cilju sigurne razmjene podatka nužnih za proces jednoznačne identifikacije korisnika od strane e-usluga. 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 NIAS-a" na kojeg se ova specifikacija direktno veže.

Tipovi subjekata koji se pojavljuju u sustavu NIAS mogu biti fizičke osobe i fizičke osobe koje djeluju unutar nekog poslovnog subjekta, prema tome razlikujemo usluge za fizičke osobe i usluge za poslovne subjekte.

Isto tako u sustavu razlikujemo osobne i poslovne vjerodajnice. Osobne vjerodajnice vraćaju podatke o fizičkim osobama, dok poslovne vjerodajnice vraćaju podatak o fizičkoj osobi i poslovnom subjektu unutar kojeg fizička osoba djeluje.

Svaka e-usluga u sustavu neovisno o tipu korisnika za koje je namijenjena mora omogućiti prijavu s osobnim ili poslovnim atributima korisnika. To znači da usluga koja je namijenjena poslovnim subjektima mora moći prihvatiti prijavu korisnika koji je fizička osoba bez poslovnih atributa.

E-usluga može koristiti i zajedničku navigacijsku traku sustava e-Građani/e-Poslovanje, te u tom slučaju NIAS autentifikacijske podatke šalje i sustavu navigacijske trake, a e-usluzi vraća autorizacijski token pomoću kojeg se usklađuje sjednica.

Informacije vezane za korisničke atribute za pojedini sustav koji je integriran u NIAS nalaze se u ovim dokumentima:

MUeH-Tehnička specifikacija korisničkih atributa za e-Građane

MUeH-Tehnička specifikacija korisničkih atributa za e-Poslovanje

Tehnička specifikacija za implementaciju jedinstvene navigacijske trake

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 u nastavku.

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. Pribavi poslužiteljski X509 certifikat (SSL certifikat) i njime zaštiti prethodno pripremljenu e-uslugu.
3. Pribavi Fina aplikacijski X509 certifikat za e-uslugu kojim će štititi komunikaciju s NIAS-om. (https://www.fina.hr/aplikativni-certifikat)
4. Preuzme javni ključ NIAS-ovog Fina aplikacijskog certifikata kojim NIAS štiti komunikaciju (link za preuzimanje: https://niastst.fina.hr/integracija/index.html#nias-certs).
5. Implementira SAML protokol 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 naziv usluge i minimalnu sigurnosnu razinu autentifikacije koju usluga zahtijeva.
7. 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.
8. Dostavi NIAS-u aplikacijski certifikat kojime predmetna usluga štiti komunikaciju s NIAS-om ali bez privatnog ključa, dakle, certifikat u .cer ili .p7b formatu.
9. Dostavi NIAS-u poslužiteljski (SSL) certifikat ali bez privatnog ključa, dakle u .cer ili .p7b formatu (potreban za zaštitu SOAP poruka).

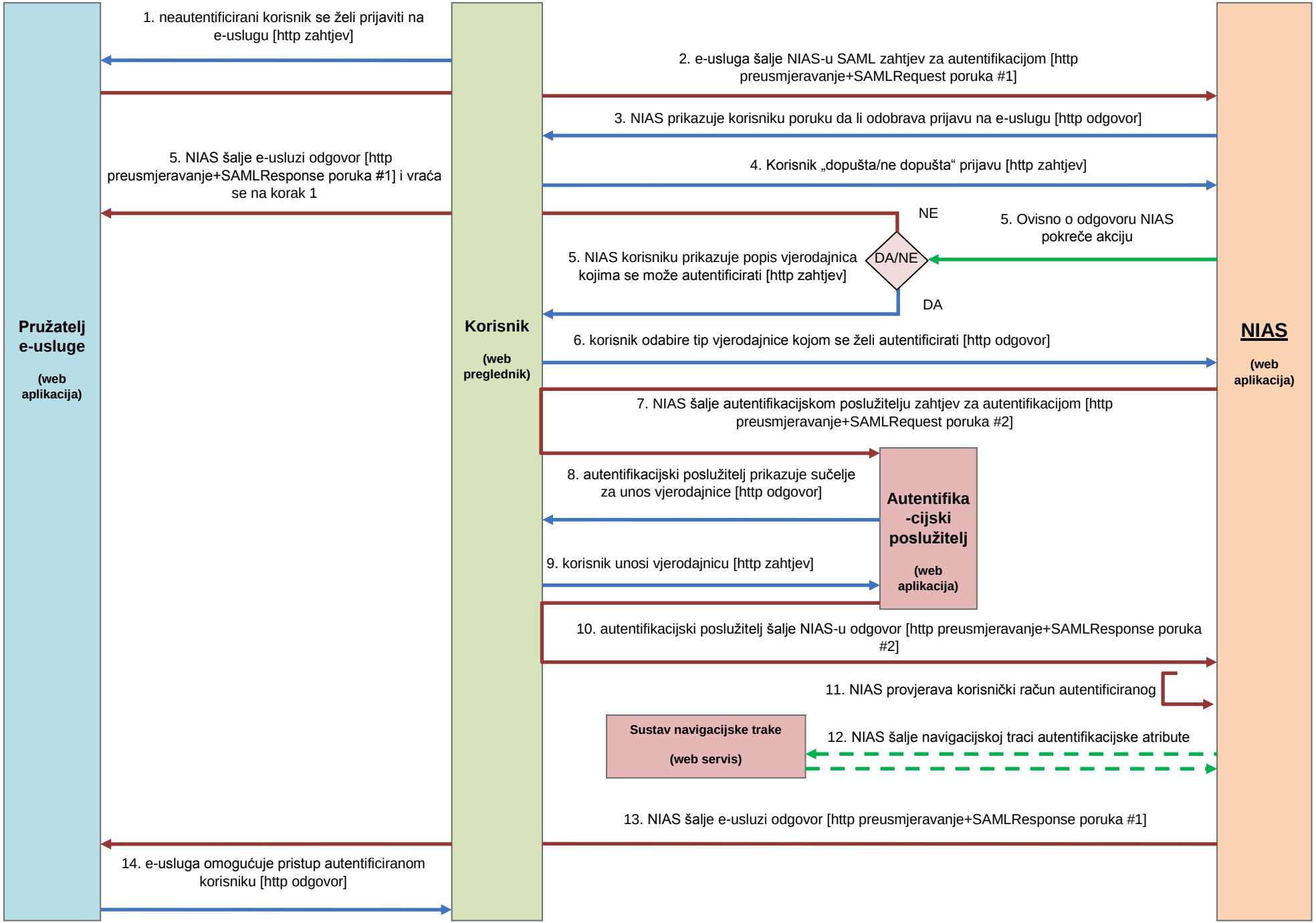
Za implementaciju SAML protokola pružatelj e-usluge može koristiti integracijske biblioteke koje nudi NIAS, integracijske biblioteke od trećih strana ili izraditi vlastite biblioteke koje podržavaju SAML standard i sadrže logiku kojom se ostvaruje veza između dva sustava.

3. Tijek komunikacije

3.1 Dijagram tijeka komunikacije SSOn

Dijagram prikazan u nastavku prikazuje tijek komunikacije između korisnika: poslužitelja elektroničke usluge, NIAS-a i autentifikacijskog poslužitelja izdavatelja vjerodajnice.

Za integraciju elektroničke usluge u NIAS nužno je da pružatelj e-usluge na poslužitelju e-usluge implementira dio SAML protokola koji omogućuje slanje SAML zahtjeva (SAMLRequest) za autentifikacijom (korak 2 u dijagramu) te zaprimanje SAML odgovora (SAMLResponse) i njegovu obradu (korak 9 u dijagramu).


Pružatelj e-usluge
(web aplikacija)
Korisnik
(web preglednik)
NIAS
(web aplikacija)
1. neautentificirani korisnik se želi prijaviti na e-uslugu [http zahtjev]
2. e-usluga šalje NIAS-u SAML zahtjev za autentifikacijom [http preusmjeravanje+SAMLRequest poruka #1]
3. NIAS prikazuje korisniku poruku da li odobrava prijavu na e-uslugu [http odgovor]
4. Korisnik „dopušta/ne dopušta“ prijavu [http zahtjev]
5. Ovisno o odgovoru NIAS pokreče akciju
NE
DA/NE
DA
5. NIAS korisniku prikazuje popis vjerodajnica kojima se može autentificirati [http zahtjev]
5. NIAS šalje e-usluzi odgovor [http preusmjeravanje+SAMLResponse poruka #1] i vraća se na korak 1
6. korisnik odabire tip vjerodajnice kojom se želi autentificirati [http odgovor]
7. NIAS šalje autentifikacijskom poslužitelju zahtjev za autentifikacijom [http preusmjeravanje+SAMLRequest poruka #2]
Autentifika-cijski poslužitelj
(web aplikacija)
8. autentifikacijski poslužitelj prikazuje sučelje za unos vjerodajnice [http odgovor]
9. korisnik unosi vjerodajnicu [http zahtjev]
10. autentifikacijski poslužitelj šalje NIAS-u odgovor [http preusmjeravanje+SAMLResponse poruka #2]
11. NIAS provjerava korisnički račun autentificiranog
Sustav navigacijske trake
(web servis)
12. NIAS šalje navigacijskoj traci autentifikacijske atribute
13. NIAS šalje e-usluzi odgovor [http preusmjeravanje+SAMLResponse poruka #1]
14. e-usluga omogućuje pristup autentificiranom korisniku [http odgovor]

Korak 1. Neautentificirani korisnik želi koristiti e-uslugu koja traži autentifikaciju te putem svojeg web preglednika pristupa na web adresu e-usluge [http zahtjev].

Korak 2. Elektronička usluga zaprimi zahtjev, provjeri identitet korisnika te, nakon što ustanovi da korisnik nije autentificiran, generira SAML zahtjev za autentifikacijom (SAMLRequest poruka #1) i preusmjerava korisnika na NIAS. SAML zahtjev za autentifikacijom, među ostalim, sadrži URL na kojem pružatelj e-usluge očekuje odgovor na zahtjev, vremenski interval valjanosti zahtjeva, certifikat za digitalno potpisivanje i certifikat za šifriranje (engl. encryption) odgovora na zahtjev te minimalnu razinu autentifikacije koju pružatelj e-usluge priznaje kao pravovaljanu za tu e-uslugu. Slanje zahtjeva na NIAS obavlja se putem korisnika na način da se korisnikov web preglednik preusmjeri na NIAS noseći pritom SAMLRequest poruku [http preusmjeravanje + SAMLRequest poruka #1].

Korak 3. Nakon što zaprimi SAML zahtjev za autentifikacijom, NIAS prikazuje korisniku poruku da je e-usluga zatražila autentifikaciju i pristup do korisničkih osobnih podataka. [http zahtjev].

Korak 4. Korisnik odabire da li dozvoljava ili ne dozvoljava prijavu i šalje NIAS-u odgovor [http odgovor].

Korak 5. **a)** NIAS zaprimi odgovor da korisnik odbija proces autentifikacije, nakon čega šalje SAML Response poruku u kojoj je obavijest o neuspješnoj autentifikaciji [http odgovor] nakon čega se korisnik preusmjerava na korak 1.

b) NIAS zaprimi zahtjev za autentifikacijom, provjeri njegovu valjanosti i nakon obrade zahtjeva korisniku prikaže popis vjerodajnica kojima se može autentificirati, a koje zadovoljavaju minimalnu zatraženu razinu autentifikacije [http zahtjev] i nakon toga ide na korak 6.

Korak 6. Korisnik iz popisa odabire tip vjerodajnice kojom se želi autentificirati [http zahtjev].

Korak 7. NIAS zaprimi odabrani tip vjerodajnice te ovisno o tipu vjerodajnice sam obavlja autentifikaciju ili preusmjerava korisnika na autentifikacijski poslužitelj. U slučaju da se za odabrani tip vjerodajnice autentifikacija obavlja na drugom autentifikacijskom poslužitelju tada NIAS generira SAML zahtjev za autentifikacijom (SAMLRequest poruka #2) i preusmjerava korisnika na odabrani autentifikacijski poslužitelj. SAML zahtjev sadrži, između ostalog, URL na kojem NIAS očekuje odgovor na zahtjev, vremenski interval valjanosti zahtjeva, certifikat za digitalno potpisivanje i certifikat za šifriranje (engl. encryption) odgovora na zahtjev. Slanje zahtjeva na autentifikacijski poslužitelj obavlja se putem korisnika na način da se korisnikov web preglednik preusmjeri na autentifikacijski poslužitelj noseći pritom SAMLRequest poruku [http preusmjeravanje + SAMLRequest poruka #2].

Korak 8. Autentifikacijski poslužitelj zaprimi zahtjev za autentifikacijom, obradi ga te korisniku prikaže sučelje za unos vjerodajnice [http odgovor].

Korak 9. Korisnik unosi svoju vjerodajnicu (korisničko ime i lozinku, certifikat i slično) i potvrđuje unos [http zahtjev].

Korak 10. Autentifikacijski poslužitelj zaprimi unesenu vjerodajnicu, provjerava je, generira SAML odgovor (SAMLResponse poruka #2 koja predstavlja odgovor na SAMLRequest poruku #2) i preusmjeri korisnika na NIAS. SAML odgovor, između ostalog, sadrži OIB autentificiranog korisnika ako je autentifikacija bila uspješna ili poruku o grešci ako nije.

Slanje odgovora na NIAS poslužitelj obavlja se putem korisnika na način da se korisnikov web preglednik preusmjeri na NIAS poslužitelj noseći pritom SAMLResponse poruku [http preusmjeravanje + SAMLResponse poruka #2].

Korak 11. NIAS zaprimi SAML odgovor autentifikacijskog poslužitelja, provjeri ga i obradi. Ukoliko zaprimljeni odgovor sadrži OIB autentificiranog korisnika tada NIAS iz OIB sustava dohvati tražene atribute korisnika.

Korak 12. Ovisno o tome je li e-Usluga integrira i zajedničku navigacijsku traku sustava e-Građani/e-Poslovanje, NIAS šalje prikupljene autentifikacijske atribute sustavu navigacijske trake. Kao odgovor dobiva autorizacijski token, kojeg će NIAS dodati u listu atributa kao rezultat autentifikacije, po kojem e-Usluga usklađuje sjednicu. Za usluge koje ne integriraju navigacijsku traku, ovaj korak se preskače. [http rest zahtjev i odgovor].

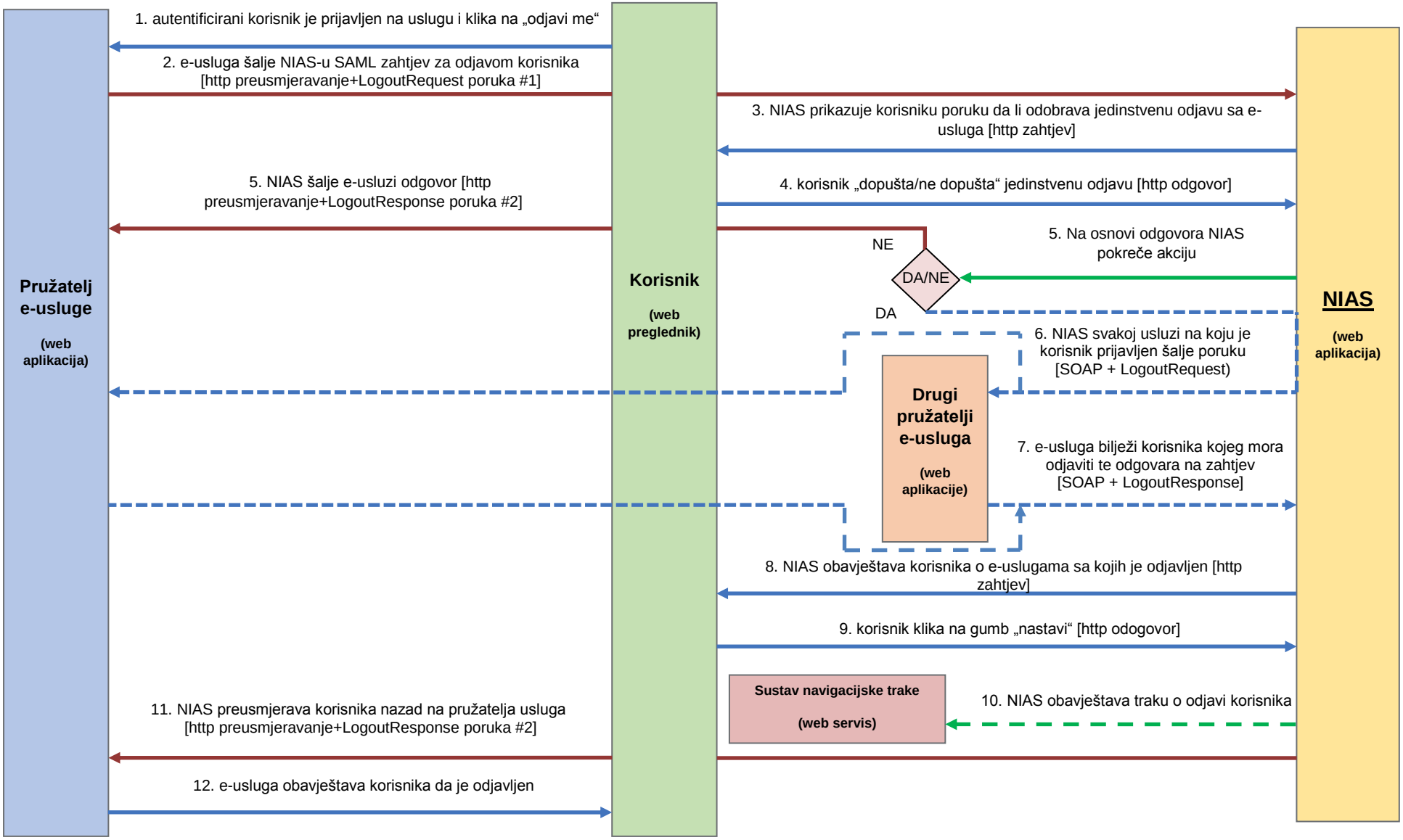
Korak 13. NIAS generira SAML odgovor (SAMLResponse poruka #1 koja predstavlja odgovor na SAMLRequest poruku #1) i preusmjeri korisnika na e-uslugu koja je tražila autentifikaciju. SAML odgovor pritom, između ostalog, sadrži tražene atribute autentificiranog korisnika ako je autentifikacija bila uspješna ili poruku o grešci ako nije. Ukoliko zaprimljeni odgovor sadrži poruku o pogrešci tada se ta poruka prikazuje korisniku i proces autentifikacije prestaje. Slanje odgovora na poslužitelj e-usluge obavlja se putem korisnika na način da se korisnikov web preglednik preusmjeri na poslužitelj e-usluge noseći pritom SAMLResponse poruku [http preusmjeravanje + SAMLResponse poruka #1].

Korak 14. E-usluga zaprimi SAML odgovor (SAMLResponse poruka #1), provjeri ga i obradi. Iz SAML odgovora e-usluga čita tražene atribute, identificira korisnika i omogućuje mu korištenje e-usluge [http odgovor].

3.2 Dijagram tijeka komunikacije SSOut

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.


Pružatelj e-usluge
(web aplikacija)
Korisnik
(web preglednik)
NIAS
(web aplikacija)
1. autentificirani korisnik je prijavljen na uslugu i klika na „odjavi me“
2. e-usluga šalje NIAS-u SAML zahtjev za odjavom korisnika [http preusmjeravanje+LogoutRequest poruka #1]
3. NIAS prikazuje korisniku poruku da li odobrava jedinstvenu odjavu sa e-usluga [http zahtjev]
4. korisnik „dopušta/ne dopušta“ jedinstvenu odjavu [http odgovor]
5. NIAS šalje e-usluzi odgovor [http preusmjeravanje+LogoutResponse poruka #2]
5. Na osnovi odgovora NIAS pokreče akciju
DA/NE
NE
DA
6. NIAS svakoj usluzi na koju je korisnik prijavljen šalje poruku [SOAP + LogoutRequest)
Drugi pružatelji e-usluga
(web aplikacije)
7. e-usluga bilježi korisnika kojeg mora odjaviti te odgovara na zahtjev [SOAP + LogoutResponse]
8. NIAS obavještava korisnika o e-uslugama sa kojih je odjavljen [http zahtjev]
9. korisnik klika na gumb „nastavi“ [http odogovor]
Sustav navigacijske trake
(web servis)
10. NIAS obavještava traku o odjavi korisnika
11. NIAS preusmjerava korisnika nazad na pružatelja usluga [http preusmjeravanje+LogoutResponse poruka #2]
12. e-usluga obavještava korisnika da je odjavljen

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 #1) 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 #1].

Korak 3. NIAS preusmjerava korisnika na stranicu na kojoj mu prikazuje poruku da li dozvoljava jedinstvenu odjavu sa svih e-usluga na koje je prijavljen [http zahtjev].

Korak 4. Korisnik odabire da li dozvoljava ili ne dozvoljava jedinstvenu odjavu i šalje NIAS-u odgovor [http odgovor].

Korak 5. **a)** NIAS zaprimi odgovor da korisnik odbija proces autentifikacije, nakon čega šalje SAML LogoutResponse poruku e-usluzi u kojoj je obavijest o neuspješnoj autentifikaciji [http odgovor] nakon čega se korisnik preusmjerava na korak 1.

b)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] i nakon toga ide na korak 6.

Korak 6. Pojedina usluga odjavljuje korisnika te odgovara na zahtjev sa SAML odgovorom LogoutResponse [SOAP + LogoutResponse].

Korak 7. 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. Klikom na link korisnik se preusmjerava nazad na e-uslugu na kojoj je korisnik zatražio odjavu. [http odgovor – http preusmjeravanje].

Korak 8. NIAS prikazuje korisniku stranicu na kojoj je popis usluga sa statusom o uspješnoj/neuspješnoj odjavi za svaku uslugu na koju je bio prijavljen [http zahtjev].

Korak 9. Korisnik na ekranu sa informacijama o jedinstvenoj odjavi klika na dugme „Nastavi" [http odgovor].

Korak 10. NIAS šalje obavijest sustavu navigacijske trake, ukoliko je potrebno, o odjavi korisnika [http rest].

Korak 11. E-usluga zaprima SAML odgovor LogoutResponse o uspješnoj odjavi [http odgovor].

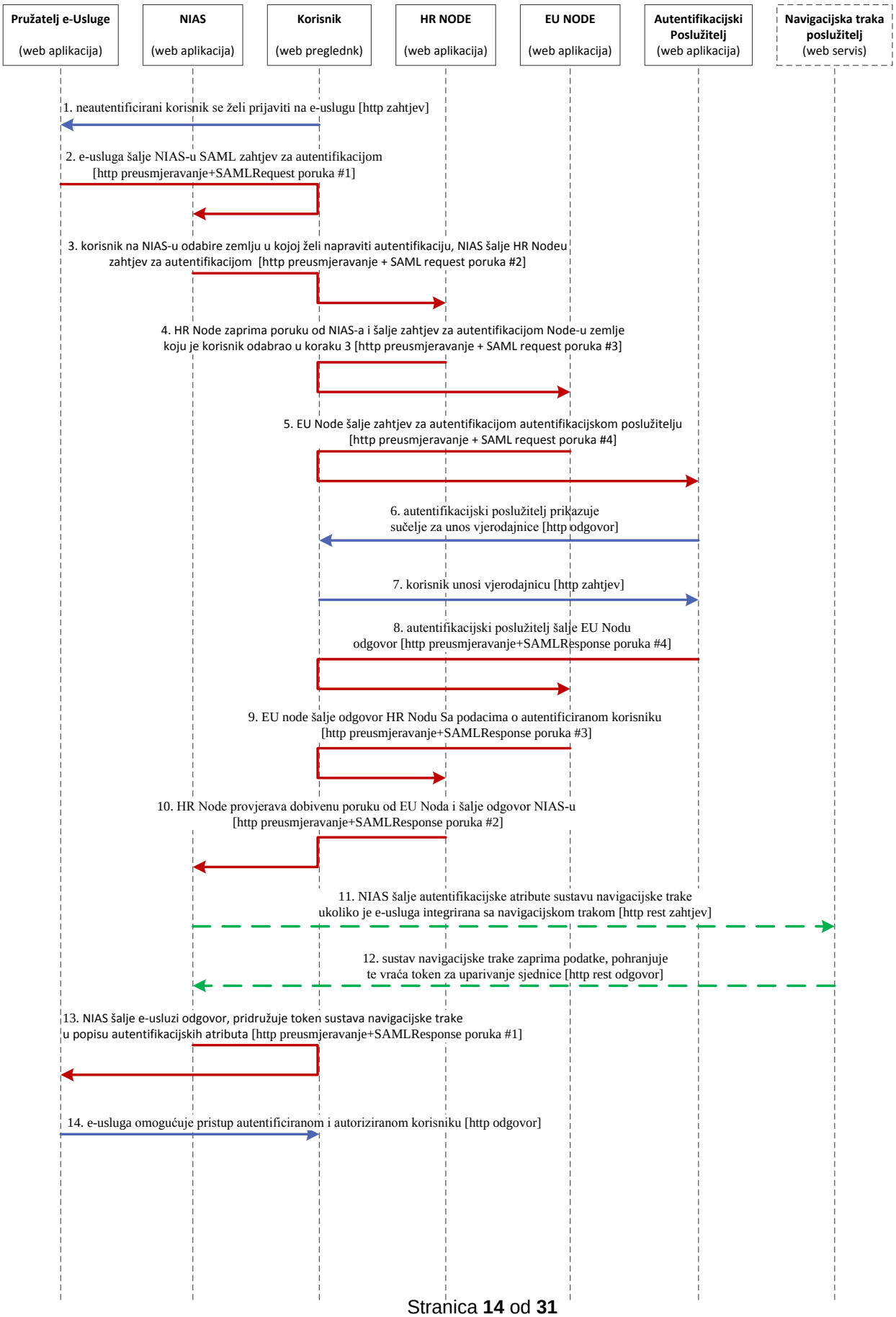
Korak 12. E-usluga prikazuje odgovarajuću poruku kako se korisnik uspješno odjavio. [http odgovor].

Napomena: e-usluga koja je zatražila LogoutRequest će biti kontaktirana zajedno sa svim ostalim e-uslugama na kojima korisnik posjeduje sjednicu tijekom koraka 5, stoga se preporuča da e-usluga odjavljuje korisnika tek prilikom koraka 5 odnosno prilikom primanja LogoutRequest poruke od NIAS-a temeljem SOAPoverHTTP protokola.

3.3 Dijagram tijeka komunikacije SSOn za Prekogranične korisnike (eIDAS)

Dijagram prikazan u nastavku prikazuje tijek komunikacije između korisnika, poslužitelja elektroničke usluge, NIAS-a, HR Noda, EU Noda i EU autentifikacijskog poslužitelja izdavatelja vjerodajnice.

Za integraciju elektroničke usluge u NIAS nužno je da pružatelj e-usluge na poslužitelju e-usluge implementira dio SAML protokola koji omogućuje slanje SAML zahtjeva (SAMLRequest) za autentifikacijom (korak 2 u dijagramu) te zaprimanje SAML odgovora (SAMLResponse) i njegovu obradu (korak 11 u dijagramu).


Pružatelj e-Usluge
(web aplikacija)
NIAS
(web aplikacija)
Korisnik
(web preglednk)
HR NODE
(web aplikacija)
EU NODE
(web aplikacija)
Autentifikacijski Poslužitelj
(web aplikacija)
Navigacijska traka poslužitelj
(web servis)
1. neautentificirani korisnik se želi prijaviti na e-uslugu [http zahtjev]
2. e-usluga šalje NIAS-u SAML zahtjev za autentifikacijom [http preusmjeravanje+SAMLRequest poruka #1]
3. korisnik na NIAS-u odabire zemlju u kojoj želi napraviti autentifikaciju, NIAS šalje HR Nodeu zahtjev za autentifikacijom [http preusmjeravanje + SAML request poruka #2]
4. HR Node zaprima poruku od NIAS-a i šalje zahtjev za autentifikacijom Node-u zemlje koju je korisnik odabrao u koraku 3 [http preusmjeravanje + SAML request poruka #3]
5. EU Node šalje zahtjev za autentifikacijom autentifikacijskom poslužitelju [http preusmjeravanje + SAML request poruka #4]
6. autentifikacijski poslužitelj prikazuje sučelje za unos vjerodajnice [http odgovor]
7. korisnik unosi vjerodajnicu [http zahtjev]
8. autentifikacijski poslužitelj šalje EU Nodu odgovor [http preusmjeravanje+SAMLResponse poruka #4]
9. EU node šalje odgovor HR Nodu Sa podacima o autentificiranom korisniku [http preusmjeravanje+SAMLResponse poruka #3]
10. HR Node provjerava dobivenu poruku od EU Noda i šalje odgovor NIAS-u [http preusmjeravanje+SAMLResponse poruka #2]
11. NIAS šalje autentifikacijske atribute sustavu navigacijske trake ukoliko je e-usluga integrirana sa navigacijskom trakom [http rest zahtjev]
12. sustav navigacijske trake zaprima podatke, pohranjuje te vraća token za uparivanje sjednice [http rest odgovor]
13. NIAS šalje e-usluzi odgovor, pridružuje token sustava navigacijske trake u popisu autentifikacijskih atributa [http preusmjeravanje+SAMLResponse poruka #1]
14. e-usluga omogućuje pristup autentificiranom i autoriziranom korisniku [http odgovor]

Korak 1. Neautentificirani korisnik želi koristiti e-uslugu koja traži autentifikaciju te putem svojeg web preglednika pristupa na web adresu e-usluge [http zahtjev].

Korak 2. Elektronička usluga zaprimi zahtjev, provjeri identitet korisnika te, nakon što ustanovi da korisnik nije autentificiran, generira SAML zahtjev za autentifikacijom (SAMLRequest poruka #1) i preusmjerava korisnika na NIAS. SAML zahtjev za autentifikacijom, među ostalim, sadrži URL na kojem pružatelj e-usluge očekuje odgovor na zahtjev, vremenski interval valjanosti zahtjeva, certifikat za digitalno potpisivanje i certifikat za šifriranje (engl. encryption) odgovora na zahtjev te minimalnu razinu autentifikacije koju pružatelj e-usluge priznaje kao pravovaljanu za tu e-uslugu. Slanje zahtjeva na NIAS obavlja se putem korisnika na način da se korisnikov web preglednik preusmjeri na NIAS noseći pritom SAMLRequest poruku [http preusmjeravanje + SAMLRequest poruka #1].

Korak 3. Nakon što zaprimi SAML zahtjev za autentifikacijom, NIAS prikazuje korisniku poruku da je e-usluge zatražila autentifikaciju te mogućnost odabira zemlje u kojoj želi napraviti autentifikaciju. Korisnik odabire zemlju i NIAS šalje SAML Request poruku HR Nodu poruku [http preusmjeravanje + SAMLRequest poruka #2].

Korak 4. HR Node zaprima poruku od NIAS-a, iz poruke uzima zemlju u kojoj se korisnik želi autentificirati i šalje zahtjev za autentifikacijom Nodu korisnika (EU Node) [http preusmjeravanje + SAMLRequest poruka #3].

Korak 5. EU Nod zaprima poruku od HR Noda i šalje zahtjev za autentifikaciju autentifikacijskom poslužitelju [http preusmjeravanje + SAMLRequest poruka #4].

Korak 6. Autentifikacijski poslužitelj zaprimi zahtjev za autentifikacijom, obradi ga te korisniku prikaže sučelje za unos vjerodajnice [http odgovor].

Korak 7. Korisnik unosi svoju vjerodajnicu (korisničko ime i lozinku, certifikat i dr.) i potvrđuje unos [http zahtjev].

Korak 8. Autentifikacijski poslužitelj zaprimi unesenu vjerodajnicu, provjerava je, generira SAML odgovor (SAMLResponse poruka #4 koja predstavlja odgovor na SAMLRequest poruku #4) i preusmjeri korisnika na EU Node [http preusmjeravanje + SAMLResponse poruka #4].

Korak 9. EU Node zaprima poruku od autentifikacijskog poslužitelja i šalje odgovor HR Nodu sa podacima korisnika. [http preusmjeravanje + SAMLResponse poruka #3].

Korak 10. HR Node zaprima poruku od EU Noda, provjeri ga i obradi, šalje odgovor NIAS-u sa podacima korisnika. [http preusmjeravanje + SAMLResponse poruka #2].

Korak 11. Ovisno o integraciji e-Usluge, ukoliko se koristi zajednička navigacijska traka sustava e-Građani/e-Poslovanje, tada NIAS dodatno šalje autentifikacijske atribute sustavu navigacijske trake. Za usluge koje ne integriraju zajedničku traku, korak 11 i 12 se preskače.

Korak 12. Sustav navigacijske trake kreira sjednicu te generira autorizacijski token za uparivanje, te vraća NIAS-u token kao odgovor. NIAS pridružuje u listi autentifikacijskih atributa i atribut nav_token.

Korak 13. NIAS vraća odgovor e-usluzi [http preusmjeravanje + SAMLResponse poruka #1].

Korak 14. E-usluga zaprimi SAML odgovor (SAMLResponse poruka #1), provjeri ga i obradi. Iz SAML odgovora e-usluga čita tražene atribute, identificira korisnika i omogućuje mu korištenje e-usluge [http odgovor].

NAPOMENA: Kod prijave prekograničnih korisnika u NIAS nema jedinstvene odjave korisnika kroz sustav NIAS. Usluga ga mora odjaviti samo kod sebe.

4. Specifikacija protokola

NIAS se temelji na razmjeni poruka između četiri različita entiteta: korisnika, pružatelja e-usluge, izdavatelja vjerodajnice 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 NIAS-a su odabrana dva protokola – HTTP-Redirect i HTTP-POST redirect binding.

4.1 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 o svojoj autentifikaciji, na ovaj je način razmjena poruka u potpunosti osigurana te su poruke nepromjenjive.

Protokol se dijeli na razmjenu poruka pomoću HTTP Redirect i HTTP POST metode.

4.2 HTTP Redirect metoda

HTTP Redirect 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. **SAMLRequest / SAMLResponse** (u ovisnosti o tome koja poruka se šalje) – SAML poruka koja je opisana kasnije u poglavlju SAMLRequest ili SAMLResponse;
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:
    - http://www.w3.org/2000/09/xmldsig#rsa-sha1
    - http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
    - http://www.w3.org/2000/09/xmldsig#rsa-sha512

    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://niaststst.fina.hr/sso-http?SAMLRequest=value&RelayState=value&SigAlg=value&Signature=value

4.3 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):

- **SAMLRequest / SAMLResponse (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 SAMLRequest / SAMLResponse poruku;
- Dodaje se skriveni <input name="RelayState"> koji sadrži vrijednost poslanu SAMLRequest porukom ili proizvoljnu vrijednosti generiranu od strane koja šalje SAMLRequest poruku.

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

URL za HTTP-POST SAML binding je: https://niaststst.fina.hr/sso-http

4.4 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 posredovanja 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>
```

5. 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).

5.1 SAMLRequest

Poruka zahtjeva 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"?>
<AuthnRequest xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ID="c831b14f-85d3-4858-
b1b0-2e7297e5177b" Version="2.0" IssueInstant="0001-01-01T00:00:00"
Destination="https://localhost/eid/authenticate.aspx"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AssertionConsumerServiceURL="https://localhost/myid/default.aspx"
xmlns="urn:oasis:names:tc:SAML:2.0:protocol">
  <Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-format:entity"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">CN=mojID, OU=FINA 00332852,
OU=Poslovni, OU=DEMO, O=FINA, C=HR</Issuer>
  <NameIDPolicy Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" />
  <Conditions NotBefore="2012-08-20T12:48:00.0771924Z" NotOnOrAfter="2012-08-
20T13:14:00.0771924Z" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <OneTimeUse />
    <Condition xmlns:q1="http://nias.eid.com.hr/2012/07/saml20Extension"
xsi:type="q1:NiasConditionType" MinAuthenticationSecurityLevel="1" />
  </Conditions>
</AuthnRequest>
```

Elementi SAMLRequest poruke su sljedeći:

- AuthnRequest kao osnovni (engl. root) element
- Issuer
- Signature
- NameIDPolicy
- Conditions

AuthnRequest 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.
- *ProtocolBinding* atribut – protokol kojim se poruka šalje. NIAS dopušta samo sljedeće protokole:
    - urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST i
    - urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect.
- *AssertionConsumerServiceURL* atribut – adresa servera koji prihvaća SAMLResponse poruku.

Issuer element:

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

NameIDPolicy element:

- *Format* atribut – odabir identifikatora kojim će korisnik biti predstavljen usluzi, NIAS podržava tri identifikatora:
    - urn:oasis:names:tc:SAML:2.0:nameid-format:persistent - korisnik je usluzi predstavljen jedinstvenim identifikatorom koji je nepromjenjiv, dvije različite usluge će imat dva različita identifikatora iste osobe
    - 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
    - urn:oasis:names:tc:SAML:2.0:nameid-format:transient - korisnik je usluzi predstavljen identifikatorom koji je promjenjiv

Conditions element:

- *NotBefore* atribut – vrijeme prije kojega SAML poruka ne vrijedi
- *NotOnOrAfter* atribut – vrijeme nakon kojega SAML poruka ne vrijedi
- *OneTimeUse* element – postojanje elementa označava da se ova poruka smije samo jednom iskoristiti. Usluga koja čita poruka u tom slučaju mora sama voditi popis svih iskorištenih ID-ova te ne dopustiti ponavljanje iste poruke. Element je u sustavu NIAS-a obavezan.
- *Condition* element – NIAS-ova ekstenzija SAML standarda koja definira atribut *MinAuthenticationSecurityLevel* pomoću kojeg se može definirati razina sigurnosti

koju usluga zahtijeva. Element nije obavezan te će se u slučaju nepostojanja tog elementa u poruci na NIAS-u upotrijebiti sigurnosna razina propisana ugovorom.

NAPOMENA: AuthnRequest poruke šalju se **HTTP Redirect** metodom

5.2 SAMLResponse

SAMLResponse (XML Response element) odgovor je na određeni zahtjev za autentifikaciju. 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"?>
<Response xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ID="f103b607-1695-4dd2-
9585-082c347dd9cb" InResponseTo="c831b14f-85d3-4858-b1b0-2e7297e5177b"
Version="2.0" IssueInstant="0001-01-01T00:00:00"
Destination="https://localhost/myid/default.aspx"
xmlns="urn:oasis:names:tc:SAML:2.0:protocol">
<Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-format:entity"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">  CN=niasaptst, OU=FINA 00332852,
OU=Poslovni, OU=DEMO, O=FINA, C=HR
</Issuer>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315" />
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <Reference URI="#f103b607-1695-4dd2-9585-082c347dd9cb">
        <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>...</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>...</SignatureValue>
    <KeyInfo>
      <X509Data>
        <X509Certificate>...</X509Certificate>
      </X509Data>
    </KeyInfo>
  </Signature>
  <Status>
    <StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    <StatusMessage>Korisnik je uspješno autentificiran.</StatusMessage>
  </Status>
```

```
  <Assertion Version="2.0" ID="48c37a4f-247c-4286-8c27-896f2a42563e"
IssueInstant="2012-08-20T12:49:33.9931924Z"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
CN=niasaptst, OU=FINA 00332852, OU=Poslovni, OU=DEMO, O=FINA, C=HR
</Issuer>
    <Subject>
      <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent">7f52aca8-0499-4f0f-bab6-e2be36716bfc</NameID>
    </Subject>
    <Conditions NotBefore="2012-08-20T12:48:33.9931924Z" NotOnOrAfter="2012-08-
20T13:14:33.9931924Z">
      <AudienceRestriction>
        <Audience>CN=mojID, OU=FINA 00332852, OU=Poslovni, OU=DEMO, O=FINA,
C=HR</Audience>
      </AudienceRestriction>
    </Conditions>
    <AuthnStatement AuthnInstant="2012-08-20T12:49:33.9931924Z"
SessionIndex="1d17314e-d05b-44f8-af01-c144057dacf9">
      <AuthnContext>
        <AuthnContextClassRef>urn:NIAS:security:level:2</AuthnContextClassRef>
      </AuthnContext>
    </AuthnStatement>
    <AttributeStatement>
      <Attribute Name="oib">
        <AttributeValue xsi:type="xsd:string">11573983273</AttributeValue>
      </Attribute>
      <Attribute Name="tid">
        <AttributeValue xsi:type="xsd:string">TID00001</AttributeValue>
      </Attribute>
     <Attribute Name="oznaka_drzave_eid">
        <AttributeValue xsi:type="xsd:string">HR</AttributeValue>
      </Attribute>
      <Attribute Name="ime">
        <AttributeValue xsi:type="xsd:string">Marko</AttributeValue>
      </Attribute>
      <Attribute Name="prezime">
        <AttributeValue xsi:type="xsd:string">Knežević</AttributeValue>
      </Attribute>
      <Attribute Name="nav_token">
        <AttributeValue xsi:type="xsd:string">f28d2b3c-4d66-4ef1-b411-1b1b2367a863-
89eb687d-77a2-4f26-bfc9-346852932e49</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</Response>
```

Elementi **SAMLResponse** poruke su sljedeći:

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

- Status;
- Assertion.

Response 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:

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

Status element, sadrži status odgovora:

- StatusCode
    - urn:oasis:names:tc:SAML:2.0:status:Success - označava uspješnu autentifikaciju;
    - urn:oasis:names:tc:SAML:2.0:status:AuthnFailed - označava da se korisnik nije uspješno autentificirao.
    - urn:oasis:names:tc:SAML:2.0:status:RequestDenied – označava da je korisnik odbio proces autentifikacije
- StatusMessage - neobavezni element sa porukom.

Assertion element sa informacijama o identitetu autentificiranog korisnika:

- Issuer – izdavatelj Assertion elementa.
- Subject – korisnik kojeg opisuje ovaj Assertion element.
- NameID – jedinstveni identifikator autentificiranog korisnika (obratiti pozornost na format jedinstvenog identifikatora, transient / persistent / entity).
- Conditions – uvjeti pod kojima ovaj Assertion element vrijedi:
    - NotBefore,
    - NotOnOrAfter,
    - AudienceRestriction.
- AuthnStatement – informacije o autentifikaciji korisnika:
    - AuthnContextClassRef – informacija o sigurnosnom nivou autentificiranog korisnika:
        - urn:NIAS:security:level:1,
        - urn:NIAS:security:level:2,
        - urn:NIAS:security:level:3,
        - urn:NIAS:security:level:4.
- AttributeStatement – popis atributa autentificiranog korisnika
    - Attribute – svaki atribut je predstavljen zasebnim elementom koji posjeduje ime i vrijednost:
        - oib, oznaka_drzave_eid, ime, prezime itd...

NAPOMENA: AuthnResponse poruke šalju se **HTTP POST** metodom

5.3 LogoutRequest

Poruka zahtjeva za autentifikacijom korisnika od drugog poslužitelja naziva se LogoutRequest 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 LogoutRequest 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="_6002844f6f70451e9b77b997c9dc5264"
               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=niasaptst, 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, jedinstveni identifikator poruke, svaka poruka mora posjedovati svoj jedinstveni identifikator. Identifikator mora biti formata *NCName*.
- *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.

NameID element:

- *Format* atribut – format indikatora kojim je prikazan identifikator korisnika, NIAS podržava tri identifikatora, usluga šalje identifikator 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.

5.4 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="_3070786e91524018b301f9e8024d90ea"
                InResponseTo="_6002844f6f70451e9b77b997c9dc5264"
                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=niasaptst, OU=FINA 00332852, OU=Poslovni, OU=DEMO, O=FINA, C=HR
  </Issuer>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-
c14n-20010315" />
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
/>
      <Reference URI="#_0ebd51b906a2473bbea4ac1e2539269b">
        <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>4vX2UyOqJdvYEuS+4qBaVoP8YVQ=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>...</SignatureValue>
    <KeyInfo>
      <X509Data>
      <X509Certificate>...</X509Certificate>
      </X509Data>
    </KeyInfo>
  </Signature>
  <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 atribut, jedinstveni identifikator poruke, svaka poruka mora posjedovati svoj jedinstveni identifikator. Identifikator mora biti formata NCName.
- 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:

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

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.

6. Specifičnosti za pružatelje e-usluga

Usluge integrirane u sustav NIAS mogu biti modificirane za prihvat više tipova osoba. Tako usluge mogu prihvatiti fizičke osobe, kako Hrvatske tako i strane državljane. Usluge isto tako mogu prihvatiti i hrvatske pravne osobe ovisno o usluzi za koji tip korisnika je namijenjena.

6.1 Specifičnosti kod jedinstvene prijave

Uloga je pružatelja e-usluge pružanje usluge korisnicima elektroničkim putem. Komunikacija s pružateljem e-usluge uvijek se odvija u istom smjeru. Zahtjev za autentifikacijom ide od e-usluge prema NIAS-u, a odgovor od NIAS-a prema e-usluzi. Pružatelj e-usluge mora implementirati logiku kojom od NIAS-a traži autentifikaciju i identifikaciju korisnika (SAMLRequest). Nakon uspješne autentifikacije, NIAS izdaje e-usluzi potvrdu o uspješnoj autentifikaciji (SAMLResponse) koja sadrži atribute autentificiranog korisnika. U slučaju neuspješne autentifikacije SAMLResponse poruka od NIAS-a u elementu StatusCode sadržavat će AuthnRequestFailed te detaljnu poruku o tome zašto korisnik nije uspješno autentificiran.

6.2 Specifičnosti kod jedinstvene odjave

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.

Ukoliko se u usluzi radi o prijavi prekograničnog korisnika tada se odjava korisnika radi na samoj usluzi. NIAS ne implementira jedinstvenu odjavu stranaca.

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

1. ***e-usluga je pokretač jedinstvene 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 jedinstvene 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).

7. Sigurnost

Protokol kojim se provodi izdavanje i prijenos poruka u sustavu NIAS osiguran je standardnim algoritmima potpisivanja – SHA1/SHA256/SHA512. Kako bi se ispravno provjerila sigurnost poruka potrebno je implementirati sljedeći algoritam provjere za SAMLRequest i SAMLResponse poruke:

- provjeriti ispravnost XML-Sig potpisa kod HTTP-POST protokola ili potpisa izvedenog iz Signature polja kod HTTP-Redirect 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.

U slučaju da je poruka tipa SAMLResponse tada je potrebno dodatno:

- 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;
- provjeriti je li poruka namijenjena e-usluzi koja je dobila poruku na način da provjeri Conditions element.