REPUBLIKA HRVATSKA
Središnji državni ured za razvoj digitalnog društva

Fina

NPIS IT

Naziv projekta: e-Poslovanje

UP.04.1.1.16.0001

PROJEKTNA DOKUMENTACIJA

„Tehnička specifikacija za integraciju vjerodajnica u NIAS“

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.

Projekt e-Poslovanje

Tehnička specifikacija za integraciju vjerodajnica u NIAS

Sadržaj

1. Uvod

Ovaj dokument ima svrhu definiranja tehničkih preduvjeta koje je nužno ispuniti da bi se ostvarila integracija izdavatelja vjerodajnica s Nacionalnim identifikacijskim i autentifikacijskim sustavom (NIAS) te ima svrhu specificiranja načina razmjene podataka između NIAS-a i izdavatelja vjerodajnica, a sve u cilju sigurne razmjene podatka nužnih za proces autentifikacije. Način razmjene podatka između NIAS-a i izdavatelja vjerodajnica 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.

2. Preduvjeti za integraciju izdavatelja vjerodajnica

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.

Izdavatelji vjerodajnice 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 ovog dokumenta.

Tehnička integracija autentifikacijskog poslužitelja izdavatelja vjerodajnice s NIAS-om obavlja se na način da izdavatelj vjerodajnice:

1. implementira proces autentifikacije korisnika svojom vjerodajnicom na autentifikacijski poslužitelj u formi web stranice dostupne putem Interneta
2. pribavi poslužiteljski X509 certifikat (SSL certifikat) i njime zaštiti prethodno pripremljenu web aplikaciju koja omogućuje autentifikaciju korisnika svojim vjerodajnicama
3. pribavi Fina aplikacijski X509 certifikat za autentifikacijski poslužitelj kojim će štititi komunikaciju s NIAS-om
4. preuzme javni ključ NIAS-ovog Fina aplikacijskog certifikata kojim NIAS štiti komunikaciju
5. implementira SAML protokol kojim se ostvaruje komunikacija između NIAS-a i autentifikacijskog poslužitelja (SAMLRequest) te autentifikacijskog poslužitelja i NIAS-a (SAMLResponse) korištenjem pribavljenog X509 aplikacijskog certifikata i porukama prema specifikaciji u nastavku
6. dostavi NIAS-u URL web stranice na kojoj izdavatelj vjerodajnice omogućuje autentifikaciju korisnika, a koja implementira SAML protokol i omogućuje zaprimanje i obradu SAMLRequest poruke od NIAS-a
7. dostavi NIAS-u aplikacijski certifikat kojim izdavatelj vjerodajnice štiti komunikaciju s NIAS-om ali bez privatnog ključa, dakle, certifikat u .cer ili .p7b formatu.

Za implementaciju SAML protokola izdavatelj vjerodajnice 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.

Poslužiteljski certifikati nisu uvjet, ali naglašeno se preporučaju klijentima NIAS-a jer se primjenom SSL protokola značajno podiže razina sigurnosti na relacijama:

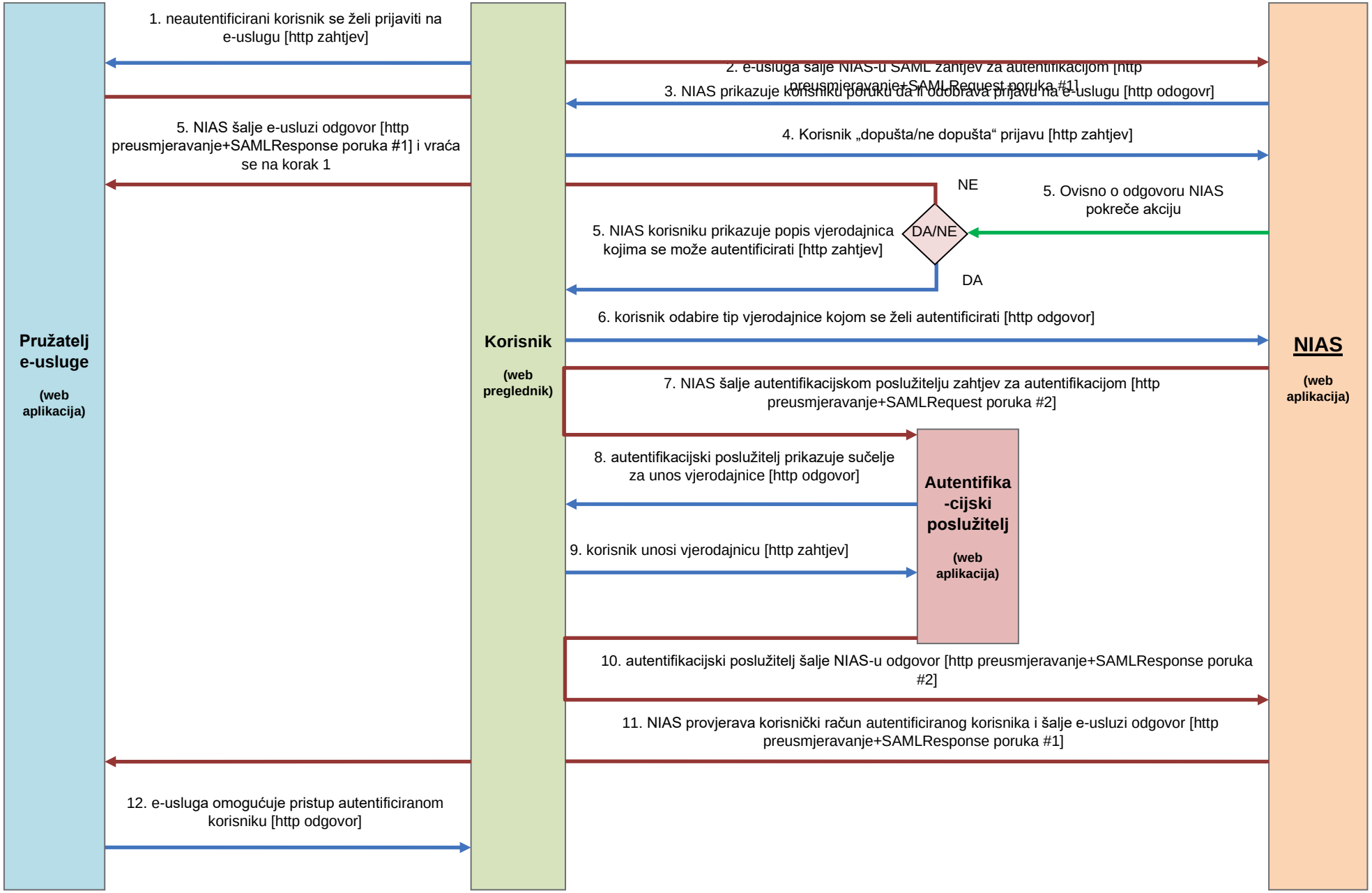
Autentifikacijski poslužitellj <–> NIAS <–> Korisnik.

2.1 Dijagram tijeka komunikacije

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 11 u dijagramu).

Za integraciju izdavatelja vjerodajnica u NIAS nužno je da izdavatelj vjerodajnica na autentifikacijskom poslužitelju implementira dio SAML protokola koji omogućuje zaprimanje SAML zahtjeva (SAMLRequest) za autentifikacijom (korak 7 u dijagramu) te slanje SAML odgovora (SAMLResponse) na NIAS poslužitelj (korak 10 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 odogovr]
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 korisnika i šalje e-usluzi odgovor [http preusmjeravanje+SAMLResponse poruka #1]
12. 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 autentifikaicjom, 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 zathjev] 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, 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 12. 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].

2.2 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.

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 nositelj 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.

2.2.2 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:

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

2.2.3 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):

- 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 sakriveni <input name="SAMLRequest"> ili <input name="SAMLResponse"> element koji sadrži Base64 enkodiranu SAMLRequest / SAMLResponse poruku;

- Dodaje se sakriveni <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 i sadržavati 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://niastst.fina.hr/sso-http

2.3 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).

2.3.1 SAMLRequest

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:

```
<AuthnRequest xmlns:xsd="http://www.w3.org/2001/XMLSchema"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
              ID="a77dc38b-d3e7-43fd-8c43-96be47c6aaeb"
              Version="2.0"
              IssueInstant="2014-10-22T07:28:30.709Z"
              Destination="https://niastst.fina.hr/finapass/samlrequest"
              ForceAuthn="true"
              ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
              Redirect
              AssertionConsumerServiceURL="https://niastst.fina.hr/Authenticatio
              n/ResponseAuthn/2"
              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>
    <NameIDPolicy Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent" />
    <Conditions NotBefore="2014-10-22T07:23:30.709Z"
                NotOnOrAfter="2014-10-22T07:33:30.709Z"
                xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
                >
        <OneTimeUse/>
    </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

2.3.2 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="8f5773a7-acd3-4fd9-a161-a77154c98828"
      InResponseTo="a77dc38b-d3e7-43fd-8c43-96be47c6aaeb"
      Version="2.0"
      IssueInstant="2014-10-22T07:29:14.514Z"
      Destination="https://niaststst.fina.hr/Authentication/ResponseAuthn/2"
      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=epasstst, 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="#8f5773a7-acd3-4fd9-a161-a77154c98828">
                <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" />
        </Status>
        <Assertion Version="2.0"
                   ID="aaff62ab-8e11-4217-abe0-12dd16d585c4"
                   IssueInstant="2014-10-22T07:29:14.514Z"
                   xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
                   >
            <Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-format:entity">
CN=epasstst, 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">e32d526b-6582-41d3-97c2-79d0696b2bab
                </NameID>
                <SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer" />
            </Subject>
            <Conditions NotBefore="2014-10-22T07:29:14.514Z"
                        NotOnOrAfter="2014-10-22T07:31:14.514Z"
                        >
                <AudienceRestriction>
                    <Audience>
CN=niasaptst, OU=FINA 00332852, OU=Poslovni, OU=DEMO, O=FINA, C=HR
                    </Audience>
                </AudienceRestriction>
            </Conditions>
            <AuthnStatement AuthnInstant="2014-10-22T07:29:14.529Z"
                            SessionIndex="96039444-fe43-420e-9ece-a06e652c4a31"
                            >
                <AuthnContext>
                    <AuthnContextClassRef>
                        urn:NIAS:security:level:2
                    </AuthnContextClassRef>
                </AuthnContext>
            </AuthnStatement>
            <AttributeStatement>
                <Attribute Name="oib">
                    <AttributeValue xsi:type="xsd:string">
                        HR1234567890
                    </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.
- 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

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

2.4 Specifikacija atributa i tipa vjerodajnica

Vjerodajnice možemo razlikovati po tipu, a postoje 2 tip vjerodajnica u NIAS-u a to su:

- **osobne vjerodajnice**
- **poslovne vjerodajnice**

2.4.1 Osobne vjerodajnice

Vjerodajnice koje se koriste za autentifikaciju fizičkih osoba u sustav NIAS, prilikom autentifikacije fizičkih osoba u sustav od vjerodajnice se očekuje da vrati **oib** atribut u SAMLResponse poruci kao identifikator fizičke osobe.

Primjer AttributeStatement elementa u SAML poruci koji sadrži atribut potreban za identifikaciju fizičke osobe

```
<AttributeStatement>
    <Attribute Name="oib">
        <AttributeValue xsi:type="xsd:string">
                1234567890
          </AttributeValue>
    </Attribute>
</AttributeStatement>
```

2.4.2 Poslovne vjerodajnice

Poslovne vjerodajnice koriste se za prijavu pravnih osoba, tj. fizičkih osoba unutar nekog poslovnog subjekta. Sustav NIAS od poslovne vjerodajnice očekuje da mu vrati sljedeće atribute u SAML Response poruci.

- oib fizičke osobe (**oib**)

- oib pravne osobe (**oib2**)
- identifikator pravne osobe (**psid**)
- dn certifkata (**dn**) – šalje se samo u slučaju da ga vjerodajnica posjeduje

atribut oib2 – poslovnog subjekta koji se prosljeđuje usluzi, a može biti oib pravne ili fizičke osobe ovisno o tipu subjekta o kojem se radi(npr. za obrte se vraća oib fizičke osobe koja je vlasnik obrta, dok se za dionička društva vraća oib tog poslovnog subjekta).

atribut psid – identifikator poslovnog subjekta koji vjerodajnica posjeduje, tako se pod ovim atributom mogu slati različiti identifikatori ovisno o tipu poslovnog subjekta

Tip poslovnog subjekta	Identifikator subjekata
Pravne osobe	MB*
Obrt	MBO*
Poljoprivredno gospodarstvo	MIBPG*
Slobodna djelatnost	MB* (DZS)
Sporedn zanimanje	RBO*

*MB – matični broj poslovnog subjekta u oib sustavu

*MBO – matični broj obrta u obrtnom registru

*MBIPG – matični identifikacijski broj poljoprivrednog gospodarstva

*MB (DZS) – matični broj slobodne djelatnosti iz državnog zavoda za statistiku

*RBO – redni broj odobrenja koji dodjeljuje Gradski ured za gospodarstvo, rad i poduzetništvo

Primjer AttributeStatement elementa u SAML poruci koji sadrži atribute potreban za identifikaciju fizičke osobe

```
<AttributeStatement>
      <Attribute Name="oib">
          <AttributeValue xsi:type="xsd:string">
            1234567890
            </AttributeValue>
      </Attribute>
      <Attribute Name="oib2">
          <AttributeValue xsi:type="xsd:string">
            85821130368
            </AttributeValue>
      </Attribute>
      <Attribute Name="ips">
          <AttributeValue xsi:type="xsd:string">
            85821130368
            </AttributeValue>
      </Attribute>
```

```
        <Attribute Name="dn">
            <AttributeValue xsi:type="xsd:string">
              SERIALNUMBER=HR22222222226.7.21, CN= HRVOJE HORVAT, G=
        HRVOJE, SN= HORVAT, L=ZAGREB, OID.2.5.4.97=HR85821130368, O=FINA,
        C=HR</AttributeValue>
        </Attribute>
    </AttributeStatement>
```

2.5 Specifičnosti za izdavatelje vjerodajnica

Uloga je izdavatelja vjerodajnice izvršavanje jednoznačne autentifikacije korisnika. Komunikacija s izdavateljem vjerodajnice uvijek se odvija u istom smjeru. Zahtjev ide od NIAS-a prema izdavatelju te odgovor od izdavatelja vjerodajnice prema NIAS-u. Izdavatelj vjerodajnice mora implementirati korisničko sučelje (npr. internetsku stranicu) koje je moguće otvoriti u skočnom (engl. pop-up) prozoru od NIAS-a te u njemu implementirati svu potrebnu logiku kako bi se korisnika jednoznačno autentificiralo. Nakon uspješne autentifikacije izdavatelj vjerodajnice mora NIAS-u izdati potvrdu o uspješnoj autentifikaciji (SAMLResponse) koja sadrži atribut/e autentificiranog korisnika. U slučaju neuspješne autentifikacije SAMLResponse poruka mora u StatusCode elementu sadržavati AuthnRequestFailed te detaljnu poruku o tome zašto korisnik nije uspješno autentificiran.

Ovisno o specifičnostima same vjerodajnice i načina rada autentifikacijskog poslužitelja definirat će se finalna izvedba integracije poštujući relevantne specifičnosti i poslovne odluke.

2.6 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 slijedeći 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.