|  |
| --- |
|  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Verzija** | **Datum** | **Opis** | **Autor** |
| A | 27.11.2015. | Odobrena inačica dokumenta |  |
| A1 | 24.7.2019 | Promjena na certifikacijskom linku |  |

Sadržaj

[1 Uvod 4](#_Toc536189931)

[1.1 Kratice i definicije 4](#_Toc536189932)

[2 CEZIH Sustav 5](#_Toc536189933)

[3 Integracija 6](#_Toc536189934)

[3.1 Sučelje web aplikacija 6](#_Toc536189935)

[3.1.1 Zahtjevi vezani uz komunikaciju preko sučelja web aplikacija 6](#_Toc536189936)

[3.1.2 Realizacija zahtjeva 7](#_Toc536189937)

[3.1.3 Integracija sa poslovnim aplikacijama 9](#_Toc536189938)

[3.1.4 Testna okolina 10](#_Toc536189939)

[3.1.5 Produkcijska okolina 11](#_Toc536189940)

[3.2 Sučelje web usluga 12](#_Toc536189941)

[3.2.1 Zahtjevi vezani uz komunikaciju preko sučelja web usluga 12](#_Toc536189942)

[3.2.2 Realizacija zahtjeva 13](#_Toc536189943)

[3.2.3 Integracija sa poslovnim servisima 18](#_Toc536189944)

[3.2.4 Greške 20](#_Toc536189945)

[3.2.5 Testna okolina 21](#_Toc536189946)

[3.2.6 Produkcijska okolina 22](#_Toc536189947)

[4 Repozitorij korisnika 22](#_Toc536189948)

[5 Grupe korisnika 23](#_Toc536189949)

# Uvod

Ovaj dokument specificira način integracije svih CEZIH aplikacija preko sigurnosnog i integracijskog sloja CEZIH sustava.

Dokumentom se opisuje proces integracije te parametri potrebni za implementaciju integracije. Detalji opisani u ovom dokumentu nadopunjuju dokument Sigurnosna Politika sa tehničkim karakteristikama značajnim za integraciju.

## Kratice i definicije

CA Certificate Authority (sustav za izdavanje digitalnih certifikata)

CEZIH Centralni Zdravstveni Informacijski sustav Republike Hrvatske

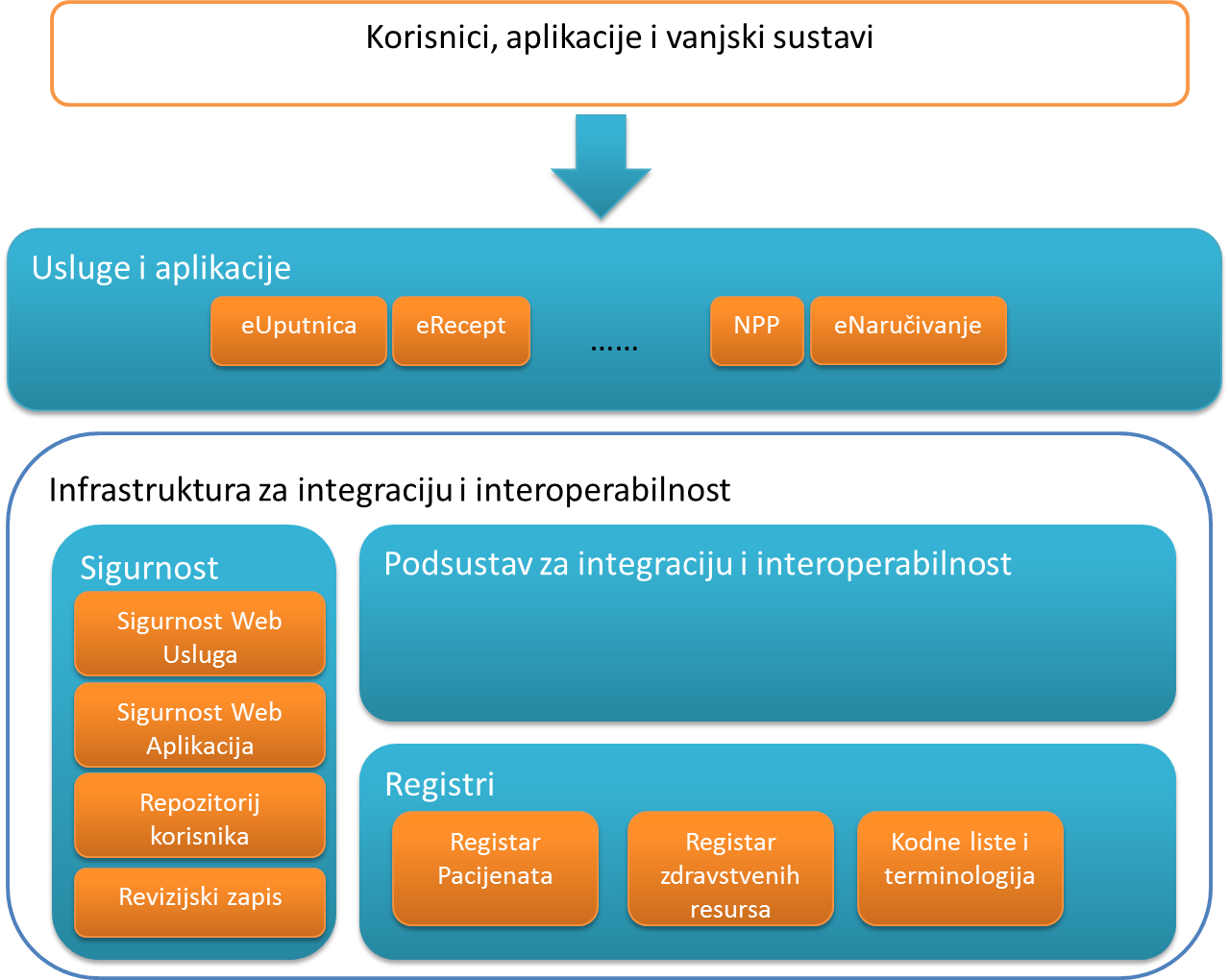
SSL Secure Socket Layer

# CEZIH Sustav

Informacijski sustav zdravstva u Republici Hrvatskoj se sastoji od niza raznih aplikacija i sustava koje su međusobno povezane putem Centralnog Zdravstvenog Informacijskog sustava Republike Hrvatske (CEZIH). CEZIH se sastoji od Infrastrukture za integraciju i interoperabilnost te aplikacija, usluga, registara i baza podataka koje su izgrađene korištenjem te infrastrukture. Kako bi se postigao najviša moguća razina sigurnosti, pouzdanosti i interoperabilnosti sve aplikacije koje se grade i implementiraju kao dio CEZIH sustava bi trebale koristiti ovu infrastrukturu.

Infrastruktura za integraciju i interoperabilnost središnjeg CEZIH sustava se sastoji od slijedećih logičkih cjelina:

* Podsustav integracije i interoperabilnosti
* Registri u zdravstvu (Registar pacijenata, Registar zdravstvenih resursa)
* Podsustav sigurnosti (Sigurnost web usluga, sigurnost web aplikacija, Revizijski zapis, Repozitorij korisnika)



Slika 1: Logičke cjeline CEZIH sustav

# Integracija

Iz perspektive CEZIH podsustava za integraciju te sigurnost, sučelja prema CEZIH sustavu možemo podijeliti u dvije skupine.

Prva skupina obuhvaća web aplikacije kojima se uglavnom pristupa koristeći web preglednik. Korisničko sučelje je realizirano u obliku web stranica. Prijavom na aplikaciju kreira se korisnička sesija na poslužiteljima.

Druga skupina obuhvaća web usluge. Web usluge su realizirane preko SOAP protokola. Klijenti web usluga su uglavnom drugi vanjski sustavi ili „standalone“ korisničke aplikacije. Svaka usluga odnosno poslana poruka se posebno autenticira i autorizira. Između pojedinih poruka ne zadržava se sesija.

Specifičnosti integracije opisani su posebno za svako sučelje u sljedećim poglavljima.

## Sučelje web aplikacija

### Zahtjevi vezani uz komunikaciju preko sučelja web aplikacija

Prilikom integracije vanjskih korisnika i sustava sa CEZIH sustavom preko web aplikacija moraju se ostvariti sljedeći zahtjevi na aplikativnom nivou:

1. Komunikacija se odvija preko šifriranog HTTPS kanala. SSL se ostvaruje uporabom serverskog certifikata izdanog od strane CEZIH CA certifikacijskog tijela. Serverski certifikat instaliran je na poslužiteljima podsustava za integraciju i sigurnost. Klijenti moraju imati ubačen CEZIH CA certifikat u svoje „trust keystore“ datoteke.
2. Prilikom uspostave HTTPS kanala odvija se „two-way handshake“, klijent se mora predstaviti koristeći X509 certifikat. X509 certifikat mora biti izdan isključivo od strane CEZIH CA certifikacijskog tijela. Za ovu namjenu mogu se koristiti osobni certifikati pohranjeni na pametnoj kartici ili aplikativni certifikati. Na ovaj način sustavu se predstavlja pošiljatelj poruke.
3. Korisnik certifikata se mora autenticirati odnosno uspješno prijaviti na sustav.
4. Korisnik koji se spaja na određenu aplikaciju mora biti autoriziran. To znači da samo korisnici sa odgovarajućom ulogom mogu pristupiti određenim aplikacijama.
5. Korisnik mora imati mogućnost odjave

### Realizacija zahtjeva

Realizacija navedenih zahtjeva implementirana je u sklopu sigurnosnog i integracijskog segmenta CEZIH sustava.

U sklopu navedenog segmenta CEZIH sustava nalaze se pristupni poslužitelji te poslužitelji za centralno upravljanje kontrolom pristupa. Prema ovim poslužiteljima ostvaruje se HTTPS konekcija.

Generalni URL za pristup prema web usluga CEZIH sustava je:

<https://web.cezih.hr/>

Sama prijava se odvija preko URL-a:

<https://sso.cezih.hr>

Ovaj URL je skriven za krajnje korisnike jer se na njega spaja u među koraku tijekom prijave na sustav pomoću certifikata. Iza ovog URL-a se kriju poslužitelji za centralno upravljanje kontrolom pristupa.

Na generalni url <https://web.cezih.hr> nastavlja se sa imenom pojedine aplikacije. Obzirom da je ovo jedinstveni ulaz preporuča se za svaku od aplikacija realizirati posebni kontekst iza imena domene. Npr:

<https://web.cezih.hr/Aplikacija1>.

Nije preporučljivo odabrati rješenje koje na poslužitelju same aplikacije neće imat kontekst aplikacije već će se pozivati kao „default“ aplikacija nakon odabira IP adrese.

Poslužitelji na osnovu korisničkog certifikata odrađuju autentikaciju i autorizaciju pošiljatelja. Autorizacija i autentikacija se izvršava na osnovu podatka o korisniku u imeničkom servisu CEZIH sustava.

Nakon što je korisnik uspješno prijavljen u CEZIH sustav, poslužitelj za kontrolu pristupa dodaje informaciju o korisniku u HTTP parametre („HTTP Header“). Informacije koje se šalju su jedinstveni identifikator korisnika iz korisnikovog certifikata (matični broj osiguranika) te set uloga koje pripadaju potpisniku. Ukoliko potpisnik sadrži više uloga svaka je odvojena zarezom od druge. Ovi podaci se dalje prosljeđuju prema „backend“ poslovnim aplikacijama.

Sljedeća tablica prikazuje primjere HTTP parametara sa imenom:

| **Naziv parametra u HTTP zaglavlju** | **Primjer vrijednosti** | **Opis** |
| --- | --- | --- |
| OAM\_REMOTE\_USER | 999999999 | Vrijednost se popunjava sa deveteroznamenkastim brojem, matični broj osiguranika |
| OAM\_REMOTE\_USER\_GROUPS | physicians, pediatrician | Vrijednost se popunjava sa ulogama kojima korisnik pripada. |

Tablica 1. HTTP parametri za web aplikacije

Jednom nakon što je korisnik prijavljen ostvaruje se sesija na poslužiteljima za kontrolu pristupa. Sesija se održava između svakog sljedećeg poziva pomoću „cookie-a“.

Ukoliko korisnik ne koristi aplikacije odnosno sesija je u neaktivnom stanju ista ističe nakon 15 minuta. Nakon toga se korisnik treba ponovno prijaviti na sustav. Obzirom da se za prijavu koristi certifikat koji je već odabran prilikom prvog spajanja ovaj postupak je neprimjetan za samog korisnika.

Preporuča se na svaku aplikaciju zaštićenu CEZIH sigurnosnim i integracijskim slojem postaviti link za odjavu. U sklopu odjave se preporuča invalidiranje sesije na samom poslužitelju aplikacije, naravno u slučaju da postoji. Nakon toga se treba preusmjeriti na link:

<https://sso.cezih.hr/centralna_odjava.html>

Spajanjem na navedeni link korisnik će biti odjavljen i sa poslužitelja za kontrolu pristupa te će mu biti prezentirana stranica o uspješnoj odjavi.

Obzirom da CEZIH „driveri“ za rad sa CEZIH karticama podržavaju samo Microsoft Crypto API moguće je koristiti preglednike koji podržavaju navedenu tehnologiju. To uključuje IE i Chrome kao preglednike koji se mogu koristiti za pristup web aplikacijama preko CEZIH sigurnosnog i integracijskoj sloja.

Obzirom da je vjerojatno da će “backend“ poslovne aplikacija biti realizirane na nekom vidu visoke dostupnosti treba naglasiti da pristupni poslužitelji nisu namijenjeni kao uređaji za balansiranje prometa. Implementacija visoke raspoloživosti treba biti realizirana na „backend“ poslužiteljima. Pristupni CEZIH poslužitelji za pojedinu aplikaciju trebaju vidjeti jednu IP adresu i jedan port.

Tijekom obrade zahtjeva pristupni serveri neće beskonačno čekati na odgovor od „backend“ aplikacije ukoliko obrada zahtjeva traje predugo. Gomilanje neobrađenih zahtjeva može uzrokovati probleme u performansama sustava. Zbog toga je na pristupnim CEZIH serverima postavljen „timeout“ od 180 sekundi. U tom vremenskom intervalu odgovor od „backend“ aplikacije mora stići. U protivnom će se korisniku vratiti greška za taj pojedini zahtjev.

### Integracija sa poslovnim aplikacijama

Prije integracije web aplikacija preko sigurnosnog i integracijskog segmenta CEZIH sustava potrebno je odraditi određene preduvjete.

Potrebno je:

1. definirati opseg korisnika koji će koristiti navedenu aplikaciju
2. definirati tehničke karakteristike klijenata (web preglednici, operativni sustav …)
3. definirati tehničke mogućnosti spajanja korisnika (VPN, IPSec, mogućnosti korištenja pametne kartice …)
4. definirati uloge koje će se koristiti u sustavu uzimajući u obzir postojeće uloge u sustavu navedene u poglavlju 5.

U fazi razvoja rješenja poslovnih usluge radi integracije sa sigurnosnim i integracijskim segmentom CEZIH-a potrebno je:

1. Definirati ime aplikacije koje će se koristiti. Primjer:

<https://web.cezih.hr/Aplikacija1>

Preporučljivo je zadržati ovakav format url-a i na „backend“ serveru web aplikacije.

Primjer:

http://{ime\_servera}:{port}/ Aplikacija1

Na taj način se smanjuje potreba za dodatnim mapiranjem ulaznih i „backend“ url-ova te se smanjuje mogućnost greške. Ukoliko postoji opravdani zahtjev za različitim ulaznim i „backend“ url-ovima može se definirati i mapiranje koje će se implementirati na integracijskom segmentu CEZIH sustava.

1. Definirati da li „backend“ aplikacija čita informaciju iz HTTP parametara o potpisniku i rolama te da li radi bilo kakve dodatne autorizacije.

Ukoliko se odrađuje dodatna autorizacija na „backend“ aplikacijama ili postoji potreba za korisničkim podacima u bazi „backend“ aplikacije, administracija i sadržaj tih podataka nije predmet ovog dokumenta. Više o repozitoriju korisnika rečeno je u poglavlju. 3.2.5.

Definirati da li aplikacija uz čitanje podatka iz HTTP Headera na osnovu njih kreira korisničku sesiju i na samoj aplikacije. Ukoliko da, potrebno je definirati na koji se način sesija ostvaruje, uporabom „cookie-a“ ili nešto treće.

1. Za potrebe testa ispravnosti konfiguracije sigurnosnog i integracijskoj segmenta CEZIH-a preporuča se izrada posebne statičke stranice koja bi bila zaštićena na isti način kao i ostatak aplikacije. Primjer URL-a takve stranice bio bi:

<https://web.cezih.hr/Aplikacija1/test>

Na stranici se može prikazati poruka o uspješnom testu sa informacijama u prijavljenom korisniku ukoliko se te informacije koriste.

Za istu namjenu može služiti i „home“ stranica, ali često se na tim stranicama već nalazi određena poslovna logika koja se počinje izvršavati što u ovom slučaju nije potrebno.

1. Sigurnosni i integracijski segment CEZIH-a će odgovore od „backend“ poslovnih aplikacija vratiti istovjetne prema klijentu. U slučaju neuspjele prijave na CEZIH vraćaju se pripadajuće stranice sa odgovarajućim informacijama i status kodovima kao što su 401, 403, 404 i slično. U slučaju internih grešaka vraća se odgovarajuća stranica sa statusom 500.
2. Implementirati link za odjavu dostupan na stranicama aplikacije kako je opisano u prethodnom poglavlju 3.1.2.
3. Ukoliko na „backend“ aplikaciji postoji korisnička sesija potrebno je uskladiti vremena trajanja sesije sa sesijom na CEZIH poslužiteljima za kontrolu pristupa. Potrebno je izbjeći slučajeve da sesija na aplikaciji istekne, a na CEZIH serverima još traje pa da prilikom spajanja na aplikaciju dolazi do greške. U tim slučajevima na aplikaciji je potrebno implementirati kreiranje nove sesije.

### Testna okolina

Nakon faze implementacije rješenja prvo se integracija treba odraditi na testnoj odnosno certifikacijskoj CEZIH okolini.

Prije same integracije potrebno je definirati:

* IP adresu poslužitelja na kojem se nalazi aplikacija
* Port poslužitelja

Za potrebe implementacije na certifikacijskoj okolini izvođač poslovne aplikacije treba instalirati istu aplikaciju. Nakon instalacije pristupit će se integraciji na CEZIH serverima.

U sklopu integracije potrebno je odraditi promjene na mrežnom nivou, ukoliko su potrebne, omogućavajući pristup između pristupnih CEZIH servera i „backend“ poslovne aplikacije.

Po uspješnoj integraciji može se pristupiti testu. Prije samog testa potrebno je definirati testne korisnike sa pripadajućim pametnim karticama i odgovarajućim ulogama. Za test se koristi testna stranica navedena u prethodnom poglavlju 3.1.2.

Pristup URL-ovima na certifikacijskoj okolini bit će analogno navedenim URL-ovima:

* <https://certweb.cezih.hr:49443>

te

* <https://certweb.cezih.hr:49443> kao link prema poslužiteljima za kontrolu pristupa

Link za odjavu na testnoj okolini je:

* [https:// certweb.cezih.hr:49443/centralna\_odjava.html](https://sso.cezih.hr/centralna_odjava.html)

Ostali podaci su istovjetni navedenima u prethodnim poglavljima.

### Produkcijska okolina

Nakon uspješne integracije i verifikacije na certifikacijskoj okolini može se odraditi implementacija na produkciji. Radovi na poslužiteljima „backend“ poslovne aplikacije mogu se odrađivati u uredovno radno vrijeme obzirom da nemaju utjecaja na ostatak produkcije i trenutnog prometa. Obzirom da pristupni serveri i serveri za kontrolu pristupa rade u produkcijskom načinu za promjene na tim serverima potrebno je definirati vremenski okvir van radnog vremena.

Prije realizacije na produkciji slično kao za certifikacijsku okolinu potrebno je definirati:

* IP adresu poslužitelja na kojem se nalazi aplikacija
* Port poslužitelja

Potrebno je odraditi propuštanja na mreži, ukoliko su potrebna, povezujući pristupne CEZIH poslužitelje sa „backend“ poslužiteljima.

Potrebno je definirati testne korisnike sa pripadajućim pametnim karticama i odgovarajućim ulogama.

Tijekom radova van radnog vremena koji će se raditi na pristupnim CEZIH poslužiteljima potrebno je osigurati dostupnost izvođača „backend“ poslovnih aplikacija. Nakon uspješne integracije i testa koristeći testnu stranicu izvođač „backend“ poslovne aplikacije treba odraditi test osnovnih funkcionalnosti potvrđujući uspješnu integraciju.

URL-ovi na produkcijskoj okolini su:

* <https://web.cezih.hr>

te

* <https://sso.cezih.hr> kao link prema poslužiteljima za kontrolu pristupa

Link za odjavu:

* <https://sso.cezih.hr/centralna_odjava.html>

## Sučelje web usluga

### Zahtjevi vezani uz komunikaciju preko sučelja web usluga

Prilikom integracije vanjskih korisnika i sustava sa CEZIH sustavom preko web usluga (web servisa) moraju se ostvariti sljedeći zahtjevi na aplikativnom nivou:

1. Komunikacija se odvija preko šifriranog HTTPS kanala. SSL se ostvaruje uporabom serverskog certifikata izdanog od strane CEZIH CA certifikacijskog tijela. Klijenti moraju imati ubačen CEZIH CA certifikat u svoje „trust keystore“ datoteke.
2. Prilikom uspostave HTTPS kanala odvija se „two-way handshake“, klijent se mora predstaviti koristeći X509 certifikat. X509 certifikat mora biti izdan isključivo od strane CEZIH CA certifikacijskog tijela. Za ovu namjenu mogu se koristiti osobni certifikati pohranjeni na pametnoj kartici ili aplikativni certifikati. Ovime se sustavu predstavlja pošiljatelj poruke.
3. Slanje poruke omogućava se samo pošiljateljima sa pripadajućom ulogom.
4. Sve poruke moraju biti u skladu sa SOAP specifikacijom. Poruke moraju biti potpisane u skladu sa WS-Security specifikacijom. Potpisivanje poruke može biti izvršeno samo sa certifikatom pohranjenim na osobnoj pametnoj kartici. Certifikati su izdani samo od CEZIH CA certifikacijskoj tijela.
5. Potpisnik poruke mora imati pravo izraditi odnosno potpisati poruku, to znači da se svaki potpisnik autorizira prilikom obrade poruke na sigurnosnom i integracijskom segmentu CEZIH sustava

### Realizacija zahtjeva

Realizacija navedenih zahtjeva implementirana je u sklopu sigurnosnog i integracijskog segmenta CEZIH sustava.

U sklopu navedenog segmenta CEZIH sustava nalaze se pristupni poslužitelji. Prema ovim poslužiteljima ostvaruje se HTTPS konekcija.

Generalni URL za pristup prema web usluga CEZIH sustava je:

[https://ws.cezih.hr:{port}/](https://ws.cezih.hr:%7bport%7d/)

Na ovaj generalni url nastavlja se sa imenom pojedinog ili skupa servisa. Novi port se definira za svaki novi skup servisa unutar pojedinog rješenja.

Poslužitelji na osnovu korisničkog certifikata odrađuju autentikaciju i autorizaciju pošiljatelja. Autorizacija i autentikacija se izvršava na osnovu podatka o korisniku u imeničkom servisu CEZIH sustava.

U nastavku obrade poruke poslužitelji prvenstveno odrađuju validaciju potpisa poruke. Ukoliko je potpis validan odrađuje se autorizacija potpisnika. Autorizacija se izvršava na osnovu podatka o potpisniku u imeničkom servisu CEZIH sustava. Detalji specifikacije WS-S navedeni su u poglavlju 3.2.2.1.

Uz validaciju potpisa poslužitelji odrađuju i validaciju poruke u odnosu na wsdl.

Nakon što je poruka uspješno obrađena isti dodaje informaciju o potpisniku u HTTP parametre („HTTP Header“). Informacije koje se šalju su jedinstveni identifikator potpisnika iz potpisnikovog certifikata (matični broj osiguranika) te set uloga koje pripadaju potpisniku. Ukoliko potpisnik sadrži više uloga svaka je odvojena zarezom od druge. Ovi podaci se dalje prosljeđuju prema „backend“ poslovnim aplikacijama.

Sljedeća tablica prikazuje primjere HTTP parametara sa imenom:

| **Naziv parametra u HTTP zaglavlju** | **Primjer vrijednosti** | **Opis** |
| --- | --- | --- |
| OAG\_REMOTE\_USER | 999999999 | Vrijednost se popunjava sa deveteroznamenkastim brojem, mbo korisnika |
| OAG\_REMOTE\_USER\_GROUPS | physicians, pediatrician | Vrijednost se popunjava sa ulogama kojima korisnik pripada. |

Tablica 2. HTTP parametri za web usluge

Obzirom da je vjerojatno da će “backend“ poslovni servisi biti realizirani na nekom vidu visoke dostupnosti treba naglasiti da pristupni poslužitelji nisu namijenjeni kao uređaji za balansiranje prometa. Implementacija visoke raspoloživosti treba biti realizirana na „backend“ poslužiteljima. Pristupni poslužitelji za pojedinu aplikaciju trebaju vidjeti jednu IP adresu i jedan port.

Tijekom obrade zahtjeva poslužitelji sigurnosnog i integracijskog segmenta CEZIH sustava neće beskonačno čekati na odgovor od „backend“ poslovnih servisa ukoliko obrada zahtjeva traje predugo. Gomilanje neobrađenih zahtjeva može uzrokovati probleme u performansama sustava. Zbog toga je na poslužitelji sigurnosnog i integracijskog segmenta CEZIH sustava postavljen „timeout“ od 180 sekundi. U tom vremenskom intervalu odgovor od „backend“ aplikacije mora stići. U protivnom će se korisniku vratiti greška za taj pojedini zahtjev.

#### Specifikacija elektroničkog potpisa poruka

Sve poruke koje se šalju prema CEZIH centralnom sustavu elektronički se potpisuju. Implementacija elektroničkog potpisa omogućava realizaciju sljedećih sigurnosnih kontrola:

* autentikacija
* integritet
* neporecivost

Svaka od navedenih kontrola implementirana je na CEZIH centralnom sustavu na razini same poruke.

Elektronički potpis realiziran je u skladu sa Web Services Security standardom odnosno njegovim dijelom vezanim uz realizaciju potpisa. WS-Security standard sam po sebi ne nudi potpunu sigurnosnu kontrolu već se nadopunjava sa ostalim kontrolama unutar same aplikacije. Primjer takve kontrole je validacija povjerljivosti sigurnosnog tokena (npr. X509 certifikata).

Struktura i elementi unutar WS-Security specifikacije definirani su sljedećim schemama:

* docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
* docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd

Sljedeća tablica prikazuje korištenje namespacea unutar WS-Security specifikacije:

|  |  |
| --- | --- |
| Prefix | Namespace |
| wsse | http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd |
| wsu | http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd |
| ds | http://www.w3.org/2000/09/xmldsig# |
| soapenv | http://schemas.xmlsoap.org/soap/envelope/ |

Tablica 3. WS-Security namespace-i

Dalje u tekstu je primjer potpisane poruke u skladu sa WS-Security standardom.

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"

xmlns:ws="https://ws.cezih.hr/">

<soapenv:Header>

<wsse:Security

xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"

xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">

<ds:Signature Id="SIG-1514194E15C0E14C3614283894613495"

xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>

<ds:CanonicalizationMethod

Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">

<ec:InclusiveNamespaces PrefixList="soapenv ws"

xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />

</ds:CanonicalizationMethod>

<ds:SignatureMethod

Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />

<ds:Reference URI="#id-1514194E15C0E14C3614283894613444">

<ds:Transforms>

<ds:Transform

Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">

<ec:InclusiveNamespaces PrefixList="ws"

xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />

</ds:Transform>

</ds:Transforms>

<ds:DigestMethod

Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

<ds:DigestValue>

pOtJt....xI8V9ehY0=

</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue>

oD4DZ+....+F9ATUk=

</ds:SignatureValue>

<ds:KeyInfo Id="KI-1514194E15C0E14C3614283894613332">

<wsse:SecurityTokenReference

wsu:Id="STR-1514194E15C0E14C3614283894613393">

<wsse:KeyIdentifier

EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"

ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3">

MIIEZjCCA06....fnKxpbLIo6QoRUOJmvbQEv0dR+vyR8=

</wsse:KeyIdentifier>

</wsse:SecurityTokenReference>

</ds:KeyInfo>

</ds:Signature>

</wsse:Security>

</soapenv:Header>

<soapenv:Body wsu:Id="id-1514194E15C0E14C3614283894613444"

xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">

<ws:Message>

<ws:elem>value</ws:elem>

</ws:Message>

</soapenv:Body>

</soapenv:Envelope>

Podaci vezani uz WS-Security unutar potpisane poruke sadržani su u *Security* elementu unutar SOAP Header elementa. Sam potpis je unutar *Signature* elementa. Postoji nekoliko generalnih opcija vezanih uz realizaciju WS-Security potpisa. Za potrebe CEZIH-a implementirana je opcija sa „detached“ potpisom unutar SOAP headera koji referencira potpisani sadržaj preko referenci na jedinstvene ID atribute pojedinog elementa.

Unutar *Security* elementa može postojati *mustUnderstand* atribut. Iz perspektive CEZIH sigurnosnog podustava i podsustava za integraciju i interoperabilnost ovaj atribut može imati vrijednost 1 ili 0. U oba slučaja će se poruke uspješno validirati te proslijediti do poslovnih servisa. Unutar implementacije pojedinih poslovnih servisa može definirati da li se i kako može koristiti *mustUnderstand* atribut*.*

Povezano s time, sigurnosni podsustav niti podsustava za integraciju i interoperabilnost ne vrše promjene na samoj poruci već je validiraju i prosljeđuju. Unutar WS-Security implementacije na CEZIH-u se ne koriste SOAP „actor/role“ elementi. U skladu s time nije preporučeno da različiti elementi brišu WS-Security blok prije konačnog odredišta odnosno konačnog poslovnog servisa.

Dalje u tekstu bit će detaljnije objašnjeni značajni elementi WS-Security segmenta te pobrojane specifičnosti CEZIH implementacije.

*SignedInfo* element sadrži informacije koje se zapravo potpisuju. Unutar tog elementa nalaze se sljedeći elementi: *CanonicalizationMethod*, *SignatureMethod* te *Reference*.

*CanonicalizationMethod* definira kanonikalizacijsku metodu kojom se dio poruke koji se potpisuje dovodi u oblik spreman za potpis. Postoje dvije opcije implementacije metoda. Za implementciju unutar CEZIH-a obvezno se mora koristiti Exclusive XML Canonicalization (xml-exc-c14n ) metoda definirana sa: [http://www.w3.org/2001/10/xml-exc-c14n#](http://www.w3.org/2001/10/xml-exc-c14n).

*SignatureMethod* postavlja algoritam kojim se vrši potpis. U slučaju CEZIH implementacije to je RSA-SHA1 definiran: <http://www.w3.org/2000/09/xmldsig#rsa-sha1>

*Reference* je element koji sadržava reference na potpisane elemente poruke. Obavezno je potpisivanje cijele poruke odnosno *Body* elementa SOAP poruke. S tim u skladu *Body* element poruke mora sadržavati atribut *Id*. Tip Id atributa mora biti definiran schemom <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd> i u skladu s time mora imati pripadajući prefix.

*Reference* element sadrži elemente *Transforms*, *DigestMethod* i *DigestValue.*

*Transforms* element definira metodu transformacije sadržaja poruke koja se potpisuje. Obavezna je upotreba koristiti Exclusive XML Canonicalization (xml-exc-c14n ) definirana sa: [http://www.w3.org/2001/10/xml-exc-c14n#](http://www.w3.org/2001/10/xml-exc-c14n) metode.

*DigestMethod* je element kojim se definira algoritam kojim se „hashira“ referencirani potpisan sadržaj.

*DigestValue* sadrži stvarnu vrijednost „hash-a“ referenciranog sadržaja. Vrijednost je base64 enkodirana.

Nakon *SignedInfo* elementa nalazi se *SignatureValue* element. Kao što mu i ime kaže ovaj element sadrži vrijednost potpisa enkodiranog u base64 obliku.

Zadnji element u WS-Security bloku je *KeyInfo*. *KeyInfo* sadržava referencu na sigurnosni token. Referenca je definirana elementom *SecurityTokenReference.*

*SecurityTokenReference* je element koji sadrži referencu na sigurnosni token potpisnika poruke. U slučaju CEZIH-a to je X509 certifikat koji sadrži javni ključ koji pripada privatnom ključu korisnika koji je potpisao poruku. Podaci o sigurnosnom tokenu nalaze se u elementu *KeyIdentifier.*

*KeyIdentifier* sadrži sam token odnosno X509 certifikat enkodiran u base64 obliku. Uz sam sadržaj sadrži atribute:

EncodingType=<http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary>

ValueType=<http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3>

Unutar CEZIH implementacije obavezna je upotreba *KeyIdentifier* elementar samog *SecurityTokenReference* elementa radi jednoznačne definicije položaja korisničkog certifikata u svrhu dodatnih validacija samog certifikata.

### Integracija sa poslovnim servisima

Prije integracije poslovnog web servisa preko sigurnosnog i integracijskog segmenta CEZIH sustava potrebno je odraditi određene preduvjete.

Potrebno je:

1. definirati opseg korisnika koji će koristiti navedene usluge
2. definirati tehničke karakteristike klijenata (krajnji korisnici koriste „stand alone“ klijente, koriste web aplikacije u sklopu centralnog rješenja ili neko treće rješenje)
3. definirati tehničke mogućnosti spajanja korisnika (VPN, IPSec, mogućosti korištenja pametne kartice …)
4. definirati uloge koje će se koristiti u sustavu uzimajući u obzir postojeće uloge u sustavu navedene u poglavlju 5.

U fazi razvoja rješenja poslovnih usluge radi integracije sa sigurnosnim i integracijskim segmentom CEZIH-a potrebno je:

1. Definirati wsdl datoteke za svaki poslovni servis. Na osnovu definiranog wsdl-a na sigurnosnom segmentu CEZIH-a može se registrirati servis.
2. Definirati potpune url-ove za poziv servisa. Preporuča se kreiranje jednog konteksta za pojedino rješenje iza kojega će dolaziti imena pojedinih servisa. Primjer:

[https://ws.cezih.hr: {port}/Rjesenje/Servis1](https://ws.cezih.hr:%20%7bport%7d/Rjesenje/Servis1)

[https://ws.cezih.hr: {port}/Rjesenje/Servis2](https://ws.cezih.hr:%20%7bport%7d/Rjesenje/Servis2)

Preporučljivo je zadržati ovakav format url-a i na „backend“ serveru poslovnog servisa.

Primjer:

http://{ime\_servera}:{port}/Rjesenje/Servis1

http://{ime\_servera}:{port}/Rjesenje/Servis2

Na taj način se smanjuje potreba za dodatnim mapiranjem ulaznih i „backend“ url-ova te se smanjuje mogućnost greške. Ukoliko postoji opravdani zahtjev za različitim ulaznim i „backend“ url-ovima može se definirati i mapiranje koje će se implementirani na integracijskom segmentu CEZIH sustava.

1. Definirati da li „backend“ poslovni servis čita informaciju iz HTTP parametara o potpisniku i rolama te da li radi bilo kakve dodatne autorizacije.

Ukoliko se odrađuje dodatna autorizacija na „backend“ servisima ili postoje potreba za korisničkim podacima u bazi poslovnog rješenja, administracija i sadržaj tih podataka nije predmet ovog dokumenta. Više o repozitoriju korisnika rečeno je u poglavlju. 3.2.5. Za potrebe testa ispravnosti konfiguracije sigurnosnog i integracijskoj segmenta CEZIH-a preporuča se definicija test operacija za svaki od poslovnih servisa. Test operacija ne bi trebala imati nikakvu povezanost sa funkcionalnošću servisa već bi samo mogla vraćati status (ok/not ok).

1. Sigurnosni i integracijski segment CEZIH-a će odgovore od „backend“ poslovnih servisa vratiti istovjetne prema klijentu. Takvi odgovori su standardni „HTTP Reponse“ kodovi i opisi grešaka. Npr, HTTP 404, 403 ili 500 sa Soap Fault-ima. prekidom konekcija i slično na CEZIH integracijskom segmentu bit će definirana SOAP Fault greška sa statusom 500 i informacijom o problemu na „backend“ poslovnom servisu. Greška je opisana u poglavlju 3.2.4 sa ostalim mogućim greškama sa sigurnosnog i integracijskoj segmenta CEZIH-a. Preporuča se da sve greške koje dolaze sa „backend“ servisa budu predefinirane te da nema grešaka sa ispisom „stack trace-a“ i slično. Takve greške trebaju biti na pravilan način prepoznate i vraćene kao interna greška sa „backend“ poslovnih servisa.

### Greške

U sljedećoj tablici pobrojane su greške koje se mogu vratiti klijentu tijekom obrade poruka na sigurnosnom segmentu CEZIH-a. Dio grešaka se vraća sa „HTTP Status Code“ 403. Te greške se vraćaju klijentu u slučaju kad nisu prošle validacije prije analize same poruke. Npr. autorizacija pošiljatelja. Drugi dio grešaka se vraća kao „SOAP Fault“ greška sa statusom 500. Te greške se vraćaju u slučajevima kad nisu prošle validacije nad samom porukom. Zadnja greška se vraća u slučaju postoji određeni interni problem na serverskoj strani koji onemogućava pravilnu obradu poruke.

|  |  |  |
| --- | --- | --- |
| **KOD** | **PORUKA** | **HTTP Status Code** |
| ERR\_SEC\_90001 | Invalid SSL Certificate | 403 |
| ERR\_SEC\_90002 | Limit Reached | 403 |
| ERR\_SEC\_90003 | Sender not authorized | 403 |
| ERR\_SEC\_90004 | Message has no Certificate in Signature | 500 |
| ERR\_SEC\_90005 | Invalid Signature Certificate | 500 |
| ERR\_SEC\_90006 | Untrusted Signature Certificate | 500 |
| ERR\_SEC\_90007 | Invalid Message Signature | 500 |
| ERR\_SEC\_90008 | No UID Attribute in Signer Certificate DN | 500 |
| ERR\_SEC\_90009 | Signer not authorized | 500 |
| ERR\_SEC\_90000 | Internal System Error | 403 |
| ERR\_SEC\_90000 | Internal System Error | 500 |

Tablica 4. Greške na sigurnosnom segmentu CEZIH-a

Tijekom obrade na integracijskom segmentu vraćaju se dva tipa grešaka. Oba tipa su „Soap Fault“ greške sa statusom 500. Jedna greška se vraća u slučaju interne greške na integracijskim poslužiteljima, druga greška se vraća u slučaju problema sa komunikacijom prema „backend“ poslovnim servisima. Sljedeća tablica prikazuje navedene greške:

|  |  |  |
| --- | --- | --- |
| **KOD** | **PORUKA** | **HTTP Status Code** |
| ERR\_EUS\_90020 | Internal System Error | 500 |
| ERR\_EUS\_90021 | Remote Service Error | 500 |

Tablica 5. Greške na integracijskom segmentu CEZIH-a

### Testna okolina

Nakon faze implementacije rješenja integracija se prvo treba odraditi na testnoj odnosno certifikacijskoj CEZIH okolini.

Pristup URL-ovima na certifikacijskoj okolini bit će analogno navedenom URL-u:

* [https://certws.cezih.hr:{port}](https://certws.cezih.hr:%7bport%7d)

Ostali podaci su istovjetni navedenima u prethodnim poglavljima.

Prije same integracije potrebno je definirati:

* IP adresu poslužitelja na kojem se nalaze poslovni servisi
* Port poslužitelja

Za potrebe implementacije na certifikacijskoj okolini izvođač poslovnih servisa treba instalirati iste servise. Nakon instalacije pristupit će se integraciji na CEZIH serverima.

Po uspješnoj integraciji može se pristupiti testu. Prije samog testa potrebno je definirati testne korisnike sa pripadajućim pametnim karticama i odgovarajućim ulogama. Za test se koristi testna operacija navedena u poglavlju 3.2.3.

### Produkcijska okolina

Nakon uspješne integracije i verifikacije na certifikacijskoj okolini može se odraditi implementacija na produkciji. Radovi na poslužiteljima „backend“ poslovnih servisa mogu se odrađivati u uredovno radno vrijeme obzirom da nemaju utjecaja na ostatak produkcije i trenutnog prometa. Obzirom da sigurnosni i integracijski segment CEZIH-a rade u produkcijskom načinu, za promjene na tim serverima potrebno je definirati vremenski okvir van radnog vremena.

Prije realizacije na produkciji slično kao za certifikacijsku okolinu potrebno je definirati:

* IP adresu poslužitelja na kojem se nalazi aplikacija
* Port poslužitelja

Potrebno je odraditi propuštanja na mreži, ukoliko su potrebna, povezujući CEZIH poslužitelje sa „backend“ poslužiteljima.

Potrebno je definirati testne korisnike sa pripadajućim pametnim karticama i odgovarajućim ulogama.

Tijekom radova van radnog vremena koji će se raditi na pristupnim CEZIH poslužiteljima potrebno je osigurati dostupnost izvođača „backend“ poslovnih aplikacija. Nakon uspješne integracije i testa koristeći testnu operaciju izvođač „backend“ poslovne aplikacije treba odraditi test osnovnih funkcionalnosti potvrđujući uspješnu integraciju.

URL na produkcijskoj okolini je:

* [https://ws.cezih.hr:{port}](https://ws.cezih.hr:%7bport%7d)

# Repozitorij korisnika

U sklopu Infrastrukture za integraciju i interoperabilnost CEZIH sustava nalazi se središnji repozitorij korisnika sustava. Ova komponenta se temelji na LDAP protokolu i sadrži sve korisnike koji imaju pravo pristupa sustavu. Podaci pohranjeni u ovom repozitoriju sadrže osnovne podatke koji su potrebni za identifikaciju korisnika te uloge koje taj korisnik ima.

Sustavi za kontrolu pristupa u sklopu infrastrukture za integraciju i interoperabilnost CEZIH sustava koriste ovaj repozitorij korisnika za identifikaciju, autentikaciju i autorizaciju korisnika i sustava koji pristupaju aplikacijama i uslugama središnjeg CEZIH sustava.

Prilikom izgradnje aplikacija i usluga CEZIH sustava trebalo bi koristiti ovaj repozitorij korisnika i podatke pohranjene u njemu u slučajevima kada aplikacija ili usluga treba unutar poslovne odnosno aplikacijske logike neke podatke o korisniku. Ti podaci mogu se proslijediti aplikaciji u obliku HTTP Headera. Ukoliko aplikacija ili usluga treba podatke kojih nema u ovom repozitoriju tada se preporuča da se u sklopu aplikacije ili usluge implementira zaseban repozitorij korisnika koji sadrži te dodatne podatke koji se koriste isključivo u sklopu te aplikacije ili usluge. Korisnici u repozitoriju aplikacije ili usluge moraju jednoznačno biti povezani sa korisnicima unutar središnjeg repozitorija korisnika Infrastrukture za integraciju i interoperabilnost CEZIH sustava korištenjem jedinstvenog identifikatora „uid“.

Administracija i sadržaj navedenih podatka trebali bi biti u svakom slučaju definirani imajući u vidu podatke u imeničkom servisu CEZIH-a. Preporuča se da se takvi podaci dobivaju iz CEZIH ZOROH baze,a nikako ne ručnom administracijom ili administracijom van okvira HZZO procesa. U takvom slučaju može doći do različitosti između podataka u imeničkom servisu i podacima o korisnicima u bazi poslovnog rješenja što vodi do grešaka i problema u radu korisnika.

# Grupe korisnika

Korisnici unutar imeničkog servisa mogu pripadati različitim grupama (ulogama). Na osnovu grupe kojoj pripada, korisniku se pridjeljuju različita prava unutar aplikacija. Popis grupa koji se trenutno nalaze su CEZIH sustavu nalazi se u HZZO dokumentaciji.