Valsts reģionālās attīstības aģentūra



|  |  |
| --- | --- |
|  |  |

Valsts informācijas sistēmu savietotāja, Latvijas valsts portāla www.latvija.lv un elektronisko pakalpojumu izstrāde un uzturēšana

3.daļa "VISS un Portāla jaunu un esošo moduļu papildinājumu izstrāde, ieviešana, garantijas apkalpošana un uzturēšana saskaņā ar tehnisko specifikāciju"

PFAS AUTH 2.Sējums

Integrācijas instrukcija un paraugi

VRAA-6\_15\_11\_58-VISS\_2010-PFAS\_AUTH\_2-II

17.08.2017. versija 1.03

Rīgā 2016

|  |  |  |
| --- | --- | --- |
|  | **IEGULDĪJUMS TAVĀ NĀKOTNĒ** |  |

Dokumenta identifikācija

|  |  |
| --- | --- |
| Dokumenta ID: | VRAA-6\_15\_11\_58-VISS\_2010-PFAS\_AUTH\_2-II-V1.03-17.08.2017. |
| Dokumenta nosaukums: | Valsts informācijas sistēmu savietotāja, Latvijas valsts portāla www.latvija.lv un elektronisko pakalpojumu izstrāde un uzturēšana.  3.daļa "VISS un Portāla jaunu un esošo moduļu papildinājumu izstrāde, ieviešana, garantijas apkalpošana un uzturēšana saskaņā ar tehnisko specifikāciju".  PFAS AUTH 2.Sējums.  Integrācijas instrukcija un paraugi. |
| Dokumenta kods: | VRAA-6\_15\_11\_58-VISS\_2010-PFAS\_AUTH\_2-II |
| Versija: | Versija 1.03, Laidiens 17.08.2017. (saīsināti V1.03 17.08.2017.) |

Saskaņojumi

|  |  |  |  |
| --- | --- | --- | --- |
| Organizācija | Vārds, uzvārds, amats | Datums | Paraksts |
| Valsts reģionālās attīstības aģentūra | Atbildīgā persona no Pasūtītāja puses |  |  |
| SIA "ABC software" | J.Korņijenko, projekta vadītājs par tehniskiem jautājumiem no Izpildītāja puses | 17.08.2017. |  |
| SIA "ABC software" | M.Pētersons, projekta vadītājs par administratīviem jautājumiem no Izpildītāja puses | 17.08.2017. |  |
| SIA "ABC software" | E.Blumberga, projekta kvalitātes kontroles vadītāja | 17.08.2017. |  |

Izmaiņu vēsture

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Versija | Datums | Apraksts | Organizācija | Autors |
| 1.00 | 05.05.2015. | Izveidota dokumenta sākotnējā versija | SIA „ABC software” | A.Zeļikovičs |
| 1.01 | 29.07.2015. | Veikti redakcionāli labojumi | SIA „ABC software” | M.Pētersons |
| 1.02 | 07.03.2016. | Pievienots PDP piemēra apraksts – aktualizēts 2. nodalījums un 2.1. nodaļa. | SIA „ABC software” | A.Mačiņš |
| 1.03 | 17.03.2017. | Papildināts PDP piemēra apraksts – 2.2. nodaļa. | SIA „ABC software” | A.Mačiņš |

**Satura rādītājs**

[Attēlu saraksts 5](#_Toc490772732)

[1. Ievads 6](#_Toc490772733)

[1.1. Dokumenta nolūks 6](#_Toc490772734)

[1.2. Darbības sfēra 6](#_Toc490772735)

[1.3. Termini un pieņemtie apzīmējumi 6](#_Toc490772736)

[1.4. Saistītie dokumenti 6](#_Toc490772737)

[1.5. Dokumenta pārskats 7](#_Toc490772738)

[2. Vispārējais apraksts 8](#_Toc490772739)

[2.1. Risinājuma pārskats 8](#_Toc490772740)

[2.2. Piemēra pārskats 8](#_Toc490772741)

[2.2.1. Priekšnosacījumi piemēra izpildei 9](#_Toc490772742)

[2.2.1.1. Pilnvaru deleģēšana 9](#_Toc490772743)

[2.2.1.2. Piemēra uzstādīšana un konfigurēšana 9](#_Toc490772744)

# Attēlu saraksts

[1.attēls. PFAS AUTH 2 PEP loģiskā shēma 8](#_Toc490772745)

# Ievads

## Dokumenta nolūks

Dokuments apraksta PFAS AUTH 2 (Juridisko personu pilnvarošanas) risinājuma biznesa loģikas izmantošanas piemērus.

Dokumentā aprakstītie piemēri ir izstrādāti ar mērķi demonstrēt pamatrisinājuma funkcionalitāti un tie nevar tikt izmantoti bez izmaiņām reālā pielietojumā.

## Darbības sfēra

Dokuments sniedz piemēru tiesību pārbaudes realizācijai pret PFAS AUTH 2 PDP (Policy decision point) XACML 2.0.

Dokuments ir paredzēts VISS sistēmu izstrādātājiem.

## Termini un pieņemtie apzīmējumi

Apzīmējumu un terminu vārdnīca pieejama dokumentā [2].

## Saistītie dokumenti

Dokuments ir izstrādāts, balstoties uz šādiem dokumentiem:

1. Valsts informācijas sistēmu savietotāja, Latvijas valsts portāla www.latvija.lv un elektronisko pakalpojumu izstrāde un uzturēšana. 3.daļa „VISS un Portāla jaunu un esošo moduļu papildinājumu izstrāde, ieviešana, garantijas apkalpošana un uzturēšana saskaņā ar tehnisko specifikāciju". PFAS AUTH 2. Programmatūras prasību specifikācija. (VRAA-6\_15\_11\_58-VISS\_2010-PFAS\_AUTH\_2-PPS).
2. „Valsts informācijas sistēmu savietotāja, Latvijas valsts portāla www.latvija.lv un elektronisko pakalpojumu izstrāde un uzturēšana”. Iepirkuma priekšmeta 3.daļa - VISS un portāla jaunu un esošo moduļu papildinājumu izstrāde, ieviešana, garantijas apkalpošana un uzturēšana saskaņā ar tehnisko specifikāciju. Terminu un saīsinājumu indekss. (VRAA-6\_15\_11\_58-VISS\_2010-TSI).
3. Valsts informācijas sistēmu savietotāja (VISS) un Vienotā valsts un pašvaldību pakalpojumu portāla www.latvija.lv pilnveidošana un uzturēšana. 3.daļa "VISS un Portāla jaunu un esošo moduļu papildinājumu izstrāde, ieviešana, garantijas apkalpošana un uzturēšana saskaņā ar tehnisko specifikāciju". PFAS AUTH 2.SĒJUMS. Programmatūras projektējuma apraksts. (VRAA-6\_15\_11\_58-VISS\_2014-PFAS\_AUTH\_2-PPA).
4. Valsts informācijas sistēmu savietotāja (VISS) un Vienotā valsts un pašvaldību pakalpojumu portāla www.latvija.lv pilnveidošana un uzturēšana. Norādījumi sertifikātu pārvaldībai. (VRAA-13\_7\_14\_50-VISS\_2014-SERT-VDL).

## Dokumenta pārskats

Dokuments sastāv no šādiem nodalījumiem:

* Dokumenta ievads – aprakstīts dokumenta nolūks, termini un pieņemtie apzīmējumi, kā arī norādīta saistība ar citiem dokumentiem un materiāliem;
* Vispārīgs apraksts – sniedz ieskatu par risinājumu funkcionalitātes izmantošanu.

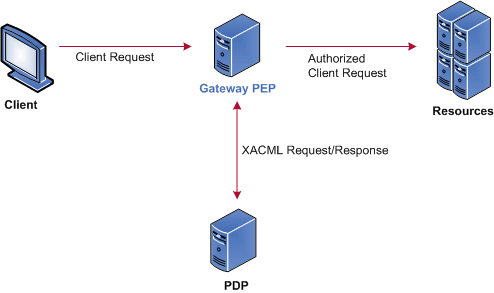
# **Vispārējais apraksts**

Pilnvarošanas risinājums ir paredzēts visām iespējamām darbībām ar pilnvarojumiem elektroniskā vidē – pilnvaras izdošana elektroniskiem resursiem (e-pakalpojumi, e-formas utt), atsaukšana un pilnvarojuma sfēras un termiņa maiņa. Pilnvarojumi tiek saglabāti PFAS autorizācijas modulī, informācija no tā tiek izmantota pieprasījumu izpildes autorizācijai. Pilnvarošanas pakalpojums paļaujas uz pilnvarošanas tiesību kontroli, izmantojot ārējus reģistrus – PMLP Iedzīvotāju reģistru un Uzņēmumu reģistru.

## Risinājuma pārskats

Pilnvarošana tehniski notiek, izmantojot latvija.lv publicēto pakalpojumu EP186 “Pilnvarojums citu e-pakalpojumu izpildei”. Ar pakalpojuma palīdzību tiek izveidota pilnvara edoc formātā un tās atspoguļojums XACML 2.0 formātā. Ārējo portālu Policy enforcement point (PEP) nodrošina tiesību pārbaudi pret PFAS AUTH 2 PDP XACML 2.0 realizāciju.

Loģiskā risinājuma shēma redzama attēlā:



1.attēls. PFAS AUTH 2 PEP loģiskā shēma

Klients veic pieprasījumu uz ārējo portālu – resurss uz kuru notika pilnvaras izdošana. Savukārt ārējā portāla PEP veic XACML pieprasījumu pret PFAS AUTH 2 PDP – lai pārliecinātos, ka lietotājam ir tiesības piekļūt resursam. Ja PDP atbild pozitīvi uz veikto pieprasījumu, ārējais portāls autorizē lietotāju piekļūt portāla resursiem.

## Piemēra pārskats

Lai veiksmīgi izpildītu piemēru, ir nepieciešams izpildīt priekšnosacījumus (skat. 2.2.1. nodaļu).

Pēc tam, kad ir izpildīti priekšnosacījumi, piemēram jābūt pieejamam: [*https://pdptest:7778/PDPClientExample45/*](https://pdptest:7778/PDPClientExample45/)(lai atvērtu, ir jāautentificējās kā fiziskai personai)*. Piebilde: tas ir būtiski, lai adrese tiešām beigtos ar slīpsvītru, t.i. https://pdptest:7778/PDPClientExample45 ir nepareiza adrese.*

Piemērs sastāv no divām daļām:

* Pilnvarotas personas autentifikācija un pārbaude pret deleģētajiem resusiem. Lai izpildītu šo piemēru, ir jāautentificējās kā pilnvarotai personai, nospiežot pogu: “autentificēties kā pilnvarotai personai”. Piemēru var izpildīt pilnvarota persona, nospiežot pogu “pārbaudīt resursus”.
* Personas pilnvaru atlasīšana (izsaucot *GetValidGrantors servisu*) un pārbade pret personai deleģētajiem resursiem (izsaucot *PolicyDecisionPoint* servisu). Piemērs izmanto autentificētās personas personas kodu (nav būtisks autentifikācijas veids). Piemēru izpilda, nospiežot pogu “atlasīt”. **NB!** *PolicyDecisionPoint* servisu **nedrīkst** izsaukt nedrošā veidā!

### Priekšnosacījumi piemēra izpildei

Lai izpildītu piemēru ir nepieciešams veikt apakšnodaļās aprakstītās darbības.

#### Pilnvaru deleģēšana

Lai deleģētu pilnvaras, ir nepieciešams: autentificēties portāla latvija.lv testa vidē (https://lvptest.vraa.gov.lv/) kā juridiskai personai, kura var vienpersoniski pārstāvēt organizāciju (valsts iestādi vai uzņēmumu); kā šādi autentificētai personai ir nepieciešams izpildīt 186. epakalpojumu, norādot nepieciešamās pilnvaras (piem., moduļu, epakalpojumu, eformu) nepieciešamai personai, norādot tās personas kodu un deleģētās pilnvaras ir jāparaksta ar laika zīmogu.

Lai veiksmīgi izpildītu piemēru, ir nepieciešams deleģēt kādu no resursiem, kas ir norādīti piemēra konfigurācijā (skat. 2.2.1.2. nodaļu). Tā kā e-pakalpojumu pilnvara ir citādāka kā citiem resursiem, tad tie ir nodalīti atsevišķi. Pēc noklusējuma piemēra konfigurācijā (*Web.config* datne) ir norādīti trīs sistēmu moduļi - *CEN*, *CEN.TEST,* *DPPS*, viena e-forma - *URN:IVIS:100001:EF.VISS-EF01-v1-0* un divi e-pakalpojumi: *URN:IVIS:100001:EP-EP500-V1-0*, *URN:IVIS:100001:EP-EP32-V1-0*.

#### Piemēra uzstādīšana un konfigurēšana

* Jābūt uzstādītam IIS 7.5, .NET 4.5.
* Jāpapildina *hosts* datne (Win8.1: *C:\Windows\System32\drivers\etc\hosts*) ar piemēra lokāli izmantoto domēnvārdu (***pdptest***), datni papildinot ar: ***127.0.0.1 pdptest***. Ja datnē jau eksistē kāds domēnvārds ***127.0.0.1*** adresei, tad ***pdptest*** *var pievienot aiz pēdējā domēnvārda, atdalot ar atstarpi*.
* Jāizveido jauns IIS lietojums ***pdptest***:
  + Lietojuma nosaukums (*site name*): ***pdptest***
  + Lietojuma pūls (*Application pool*): noklusētā vērtība (***pdptest***)
  + Jānorāda pilnais ceļš uz piemēra atarhivētā arhīva apakškatalogu ***Empty*** (*physical path*)
  + Lietojums jānokonfigurē tā, lai tas izmantoto ***HTTPS*** prototoku (*binding*) ar ***7778*** portu (*port*)
  + Kā resursdatora nosaukums (*Host name*) jānorāda ***pdptest.***
* Izveidotajam lietojumam jānorāda derīgs SSL sertifikāts (var būt pašparakstīts) skat. [4] dokumenta 3.7. nodaļu. Ja nav neviena derīga SSL sertifikāta, tad skat. [4] dokumenta 3.2. nodaļu.
* Izveidotā IIS lietojuma pūlam jāpiešķir lasīšanas tiesības lietojuma katalogam: IIS manager -> nospiežam uz IIS lietojuma -> izvēlamies “*Edit Permissions*” (labajā pusē) -> security -> edit -> add -> location -> lokālais dators -> OK -> ievadām IIS pūla lietotāju (IIS APPPOOL\pdptest) -> nospiežam *check name*, ja lietotāju atrod, tad spiežam OK. (Piezīme1: tā kā šis ir piemērs, tad tiesības varam piešķirt atarhivētā piemēra katalogam (*PDP\_ClientExample*), tad tās būs jāpiešķir tikai vienreiz)
* Jāizveido IIS apakšlietojums ***pdptest*** lietojumam:
  + Kā *alias* jānorāda ***PDPClientExample45***
  + Jānorāda pilnais ceļš uz piemēra atarhivētā arhīva apakšakatalogu ***PDPClientExample45*** *(****piemēram, C:\Dev\NET\Pilnvaru tests\PDPClientExample\PDPClientExample45****)*
  + IIS lietojuma pūlam jāpiešķir lasīšanas tiesības izveidotā IIS apakšlietojuma katalogam (līdzīgi kā IIS lietojumam).
* Jāuzstāda piemēra arhīva kataloga ***Certificates*** apakškatalogā esošais ***pdp-test.pfx*** sertifikāts zem ***Local Machine/Personal*** (skat. [4] dokumenta 3.3. nodaļu):
  + Izveidotā IIS lietojuma pūlam jāpiešķir tiesības lasīt uzstādītā sertifikāta privāto atslēgu skat. [4] dokumenta 3.4. nodaļu.
* Lai tiktu rakstīti pilno kļūdu logi, nepieciešams *Web.config* datnes system.diagnostics sekcijā norādīt katalogus, kur saglabāt logu failus un *IIS* lietojuma aplikāciju pūlam jāpiešķir tiesības rakstīt attiecīgajos katalogos.
* Piemērā izmantotie pilnvarojamie resursi un e-pakalpojumi ir konfigurējumi *Web.config* datnes *appSettings* sekcijas parametros - attiecīgi *ResourcesCommaSeparedList* un *EservicesCommaSeparedList*, kur tie (resursu vai epakalpojumu identifikatori) ir jānorāda atdalīti ar komatiem (bez atstarpēm).