Valsts reģionālās attīstības aģentūra



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

Vienotā pieteikšanās: ārējās saskarnes apraksts

Programmatūras projektējuma apraksts

VRAA-VP-AS

18.01.2013. versija 1.01

Rīgā 2013

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

Dokumenta identifikācija

|  |  |
| --- | --- |
| Dokumenta ID: | VRAA-VP-AS-PPA-V1.01-18.01.2013. |
| Dokumenta nosaukums: | Vienotā pieteikšanās: ārējās saskarnes apraksts.  Programmatūras projektējuma apraksts. |
| Dokumenta kods: | VRAA-VP-AS-PPA |

Izmaiņu vēsture

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Versija | Datums | Apraksts | Organizācija | Autors |
| 0.1 | 03.04.2013. | Izveidota dokumenta sākotnējā versija | Valsts reģionālās attīstības aģentūra | R.Zirnītis |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Satura rādītājs

[1Ievads 5](#__RefHeading__1091_1145401416)

[1Dokumenta nolūks 5](#__RefHeading__1093_1145401416)

[2Darbības sfēra 5](#__RefHeading__1095_1145401416)

[3Termini un pieņemtie apzīmējumi 5](#__RefHeading__1097_1145401416)

[4Saistītie dokumenti 5](#__RefHeading__1099_1145401416)

[5Dokumenta pārskats 6](#__RefHeading__1101_1145401416)

[2Konkrētās prasības 7](#__RefHeading__1103_1145401416)

[1Vienotās pieteikšanās darbības apraksts 7](#__RefHeading__1105_1145401416)

[1Solis Nr.2 Drošības talona pieprasījums 7](#__RefHeading__1107_1145401416)

[2Solis Nr.5 – Drošības talona izsniegšana 8](#__RefHeading__1109_1145401416)

[3Solis Nr.6 – SAML apgalvojuma pārbaude 8](#__RefHeading__1111_1145401416)

1. Ievads

VP ir e-pakalpojums, kuru VRAA sniedz valsts un pašvaldību iestādēm un kurš nodrošina personas autentifikācijas uzsākšanas iespēju kredītiestāžu informācijas sistēmās un kredītiestāžu informācijas sistēmās autentificētu kredītiestāžu klientu datu (vārds, uzvārds un personas kods) nodošanu e-pakalpojumu portālam, kurš ir iniciējis VP.

VP ir uz apgalvojumiem bāzētas identitātes modulis (The Claims-Based Identity Model) [2].

VP ir veidota uz WS-Federation arhitektūras pamata, kas nodrošina elastīgu vienotas identitātes arhitektūru, kas skaidri definē un nodala uzticības mehānismus, drošības talona formātus un protokolus talonu (token) iegūšanai. Šī arhitektūra nodrošina vairākkārt izmantojamu drošības talonu servisa modeli un protokolu, kurš nodrošina identitātes noskaidrošanai nepieciešamo pieprasījumu adresēšanu gan web aplikāciju, gan web servisu līmenī visdažādākajās kombinācijās[3]. VP ietvaros var tikt izmantots izmantots WS-Federation V1.2 [1].

VP pamatā tiek izmantots WS-Federation pasīvas autentifikācijas modelis (WS-Federation: Passive Requestor Profile) [4]. Šī modeļa ietvaros gala rezultātā VP izsniedz drošības talonu – SAML apgalvojumu [5].

* 1. Dokumenta nolūks

Dokuments nosaka prasības VP funkcionalitātei, kas kā serviss būs pieejams valsts un pašvaldību iestāžu e-pakalpojumu portāliem.

Šis dokuments ir paredzēts:

* VRAA pārstāvjiem, kuri uztur VP;
* Valsts un pašvaldību iestādēm, kuras savos e-pakalpojumu portālos plāno integrēt VP, kā arī šo iestāžu izstrādātājiem.
  1. Darbības sfēra

Dokuments ir izmantojams VP izmantojošo e-pakalpojumu portālu funkcionalitātes izstrādei.

* 1. Termini un pieņemtie apzīmējumi

VRAA – Valsts reģionālās attīstības aģentūra

VP – VRAA sniegtais autentifikācijas pakalpojums „Vienotā pieteikšanās”

PS – valsts vai pašvaldību iestāde, kura no savas tīmekļa vietnes izsauc VP

AS – autentifikācijas sniedzējs, kurš VRAA nodrošina Lietotāja autentifikāciju autentifikācijas sniedzēja lietojumā un nosūta VRAA autentificētā Lietotāja personas datus.

Lietotājs – PS e-pakalpojumu lietotājs PS tīmekļa vietnē.

* 1. Saistītie dokumenti

Dokuments ir izstrādāts, balstoties uz šādiem dokumentiem:

1. <http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html>
2. <http://msdn.microsoft.com/en-us/library/ee517291.aspx>
3. <http://msdn.microsoft.com/en-us/library/bb498017.aspx>
4. http://msdn.microsoft.com/en-us/library/bb608217.aspx
5. https://ivis.eps.gov.lv/IVIS.LVP.STS/FederationMetadata/2007-06/FederationMetadata.xml/
   1. Dokumenta pārskats

Dokuments sastāv no 2 nodalījumiem:

* Dokumenta ievads – aprakstīts dokumenta nolūks, termini un pieņemtie apzīmējumi, kā arī norādīta saistība ar citiem dokumentiem un materiāliem;
* Konkrētās prasības – VP procesa aprakstu, VP izsaukšanu, drošības talona izsniegšanu un drošības talona pārbaudi.

1. Konkrētās prasības
   1. Vienotās pieteikšanās darbības apraksts



| Nr. | Solis | Kas veic | Apraksts |
| --- | --- | --- | --- |
| 1. | Nospiež pogu „”Vienotā pieteikšanās” | Tīmekļa pārlūks | Ārējā PS tīmekļa vietnē Lietotājs pieprasa piekļūt PS aizsargātam resursam. Lietotājs nav autentificējies tīmekļa vietnē. Tīmekļa pārlūks pieprasījumu redirektē PS serverim, lai PS serveris, kurš ir atbildīgs par lietotāju identitātes pārvaldību PS pusē, uzņemtos autentifikācijas procesa vadību. |
| 2. | Drošības talona pieprasījums | PS | PS ģenerē drošības talona pieprasījumu un redirektē tīmekļa pārlūku uz VP moduli. |
| 3 | Tīmekļa lapas attēlošana | VP | 1. VP modulis attēlo VP tīmekļa lapu, no kuras pēc Lieotāja izvēles attiecīgajam AS pieprasa autentifikāciju (saņemt Lietotāja personas datus) AS lietojumā un pārvirza tīmekļa pārlūku uz atbilstošā AS tīmekļa lapu. |
| 4 | Lietotāja personas datu iegūšana | AS | Lietotājs autentificējas Autentifikācijas sniedzēja lietojumā.  AS autentifikācijas procesa ietvaros iegūtos Lietotāja personas datus nosūta VP modulim un pārvirza tīmekļa pārlūku atpakaļ uz VP. |
| 5 | Drošības talona izsniegšana | VP | VP modulis, izmantojot no AS saņemtos Lietotāja personas datus, ģenerē drošības talonu, kurš satur parakstītu SAML apgalvojumu.  Drosības talons caur POST metodi tiek nosūtīts PS un tīmekļa pārlūks tiek pārvirzīts uz PS norādīto tīmekļa lapu. |
| 6 | SAML apgalvojuma pārabaude | PS | PS pārbauda, vai SAML apgalvojuma paraksts un pats apgalvojums ir derīgs. Ja paraksts un apgalvojums ir derīgs, tad PS Lietotājam izveido sesiju un tīmekļa pārlūku pārvirza uz pieprasīto resursu. |

* + 1. Solis Nr.2 Drošības talona pieprasījums

|  |  |  |  |
| --- | --- | --- | --- |
| Identifikators | IdentitySelectorStart | | |
| Nosaukums | Drošības talona pieprasījums | | |
| Ievads | | | |
| Šajā sadaļā tiek aprakstīti obligātie parametri, kuri PS jānorāda, lai veiktu atbilstošu drošības talona pieprasījumu, izmantojot WS-Federation V1.2 protokolu [1]. | | | |
| Ievaddati | | | |
| Nosaukums | Tips | obligāts | Apraksts |
| Parametrs saskaņā ar [2] dokumenta 13.2.nodaļu | Parametrs saskaņā ar [2] dokumenta 13.2.nodaļu | Parametrs saskaņā ar [2] dokumenta 13.2.nodaļu | Parametrs saskaņā ar [2] dokumenta 13.2.nodaļu |
| Izvaddati | | | |
| Nosaukums | Tips | Apraksts | |
| Drošības talons | XML | VP izsniegtais drošības talons kā SAML apgalvojums. | |

* + 1. Solis Nr.5 – Drošības talona izsniegšana

|  |  |  |  |
| --- | --- | --- | --- |
| Identifikators | IdentitySelectorAnswer | | |
| Nosaukums | Drošības talona izsniegšana | | |
| Ievads | | | |
| VP izveido un PS nosūta drošības talonu. Drošības talons VP gadījumā ir SAML apgalvojums [5].  Šajā nodaļā minēti SAML apgalvojumā iekļautie atribūti, kas raksturo AS lietojumā autentificētā Lietotāja personas datus, kā arī pašu AS. | | | |
| Ievaddati | | | |
| Nosaukums | Tips | obligāts | Apraksts |
| issuer | String | Jā | Drošības talona izsniedzēja identifikators. Iespējamā vērtība kā konstante: <http://www.latvija.lv/trust>. |
| privatepersonalidentifier | String | Jā | AS lietojuma izsniegtais autentificētā Lietotāja personas kods. |
| givenname | String | Jā | AS lietojumā autentificētā Lietotāja vārds |
| surname | String | Jā | AS lietojumā autentificētā Lietotāja uzvārds |
| 109x34 | URL | Jā | AS logo (PNG datnes formātā) atrašanās vietas adrese. |
| AuthenticationMethod | string | Jā | AS identifikators, kurš autentificēja Lietotāju.  Identifikators tiek veidots šādā formātā:  URN:IVIS:100001:AM-PAREX |
| Izsaucamās prasības | Nosaukums | Izvaddati (izsaucamās prasības ievaddati) | |
| Nav |  |  | |
| Izvaddati | | | |
| Nav | | | |

* + 1. Solis Nr.6 – SAML apgalvojuma pārbaude

|  |  |
| --- | --- |
| Identifikators | ValidateSaml |
| Nosaukums | PS pārbauda saņemto drošības talonu (SAML apgalvojumu) |
| Ievads | |
| PS atbildība ir pirms Lietotāja pielaides aizsargātajam resursam, veikt drošības talona pārrbaudi. | |
| Ievaddati | |
| * Nav | |
| Apstrāde | |
| 1. Drošības talona pārbaudei PS veic šādas darbības:    1. Veic drošības talona atšifrēšanu – tikai, ja drošības talons ir šifrēts. WS-Federation v1.2. protokola ietvaros VP pusē tiek nodrošināta drošības talona šifrēšana, izmantojot PS sertifikāta publisko daļu (publisko atslēgu). Drošības talona atšifrēšanu PS veic, izmantojot sertifikāta privāto daļu (privāto atslēgu).    2. Pārbauda sertifikātu, kurš izmantots VP sūtītā drošības talona parakstīšanai:       1. Vai sertifikāts ir uzticams?;       2. Vai sertifikātu izdevis atbilstošais CA?;    3. Pārbauda drošības talona parakstu (Siganture);    4. Pārbauda drošības talona derīguma termiņu (Created, Expires);    5. Pārbauda, vai talons ir izsniegts priekš PS (Audience)    6. Tikai pēc tam nolasa drošības talonā iekļautos Lietotāja personas datus – vārdu, uzvārdu un personas kodu. Ja PS neveic drošības talona pārbaudi, tad PS uzņemas pilnu atbildību par sekām, kas no tā var iestāties. | |