SECURITY SOLUTIONS FOR E-SERVICE SYSTEMS

РЕШЕНИЯ БЕЗОПАСНОСТИ В СИСТЕМАХ Е-УСЛУГ

DROŠĪBAS RISINĀJUMI E-PAKALPOJUMU SISTĒMĀS

E. Žeiris, M. Ziema

Atslēgas vārdi: e – pakalpojums, e – pakalpojuma drošības sistēmas arhitektūra, drošības sistēmas arhitektūras izveide, konfidencialitāte, integritāte, pieejamība, autentifikācija, autorizācija.

1. E – pakalpojumu drošība

Bieži vien ar informācijas sistēmu drošību saprot tikai informācijas konfidencialitāti, bet drošības jēdziens ir daudz plašāks. Informācijas sistēmu drošība ietver šādas sastāvdaļas:

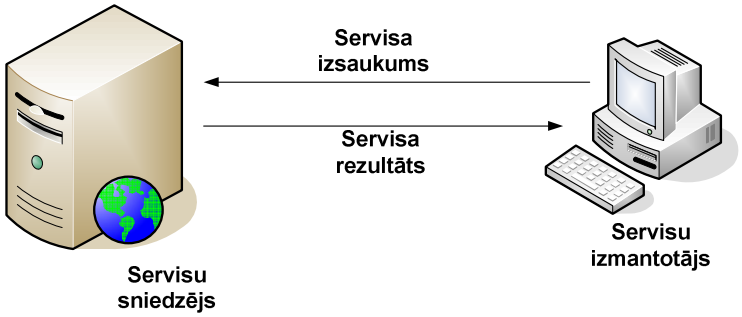
- konfidencialitāte – tikai un vienīgi autorizētu lietotāju piekļuve datiem;
- integritāte – aizsardzība pret neautorizētu datu papildināšanu un datu veselumu;
- pieejamība – tiek nodrošināta pieeja datiem un sistēmām autorizētiem lietotājiem, kad tas ir nepieciešams.

Lai izveidotu drošības sistēmas arhitektūru jebkāda veida informācijas sistēmā, ir nepieciešams veikt drošības politikas definēšanu un iespējamo risku modelēšanu. Drošības politikas definēšana ir atkarīga no organizācijas, kam paredzēta informācijas sistēma, kā arī no pašas informācijas sistēmas un tās mērķiem. Informācijas sistēmas iespējamo risku modelēšanai un identificēšanai ir iespējams pielietot dažādas metodes, kas ir standartizētas[1].

E-pakalpojumu sistēmas ir īpatnējas ar to, ka tās ir modulāras, kā arī procesi bieži vien notiek asinhroni. Pakalpojumu izpilde tiek sadalīta pa soļiem, kas nozīmē, ka drošība ir jānodrošina katrā modulī un katrā no pakalpojuma izpildes soļiem. E-pakalpojums ir paredzēts plašam klientu lokam. Tas nozīmē, ka ir jārisina klientu autentifikācijas un autorizācijas problēmas.

Aplūkosim, kādai tad vajadzētu būt e-pakalpojumu drošības sistēmai. Atkarībā no pakalpojuma veida var būt dažāda līmeņa drošības prasības. Tas nozīmē, ka viens no nosacījumiem drošības sistēmas izveidē ir tās pielāgojamība atkarībā no pakalpojuma, lai netiktu mazināta veiktspēja un nepalielinātos izmaksas uz drošības rēķina, jo lielāka drošība prasa lielākus resursus. Viens no e-pakalpojuma mērķiem ir tā pieejamība jebkuram klientam. Kamēr valstī nav ieviests elektroniskais paraksts, tikmēr ir jārisina klientu autentifikācijas problēma. Līdz ar to drošības sistēmai ir jāspēj identificēt klientus, kas reģistrēti dažādos reģistros, lai paplašinātu e-pakalpojuma izmantojamību un pieejamību. Ja runā par pakalpojuma pieejamību, tad ir nepieciešams nodrošināt tā darbību praktiski 7x24 stundas nedēļā, kas arī uzliek savus nosacījumus drošības sistēmai. Ir jāpiemin arī e-pakalpojumu konfidencialitāte, lai nenotiktu informācijas noplūde, un integritāte, lai klienta izvēlētais pakalpojums tiktu izpildīts un sasniegts gaidāmais rezultāts.

Ja runājam par e-pakalpojumiem, tad drošība noteikti ir jāaplūko servisu orientētas arhitektūras kontekstā (SOA), jo e-pakalpojumus veido SOA. SOA pēc savas būtības ir servisu kopa – viens vai vairāki servisi, kuriem tiek nodoti vai saņemti dati un kurus secīgi izsauc klients (1. attēls). Katrs serviss sevī satur pēc iespējas pilnu funkcionalitāti, kas nav atkarīga no citu servisu stāvokļa vai konteksta.



1. attēls. Servisu orientēta arhitektūra.

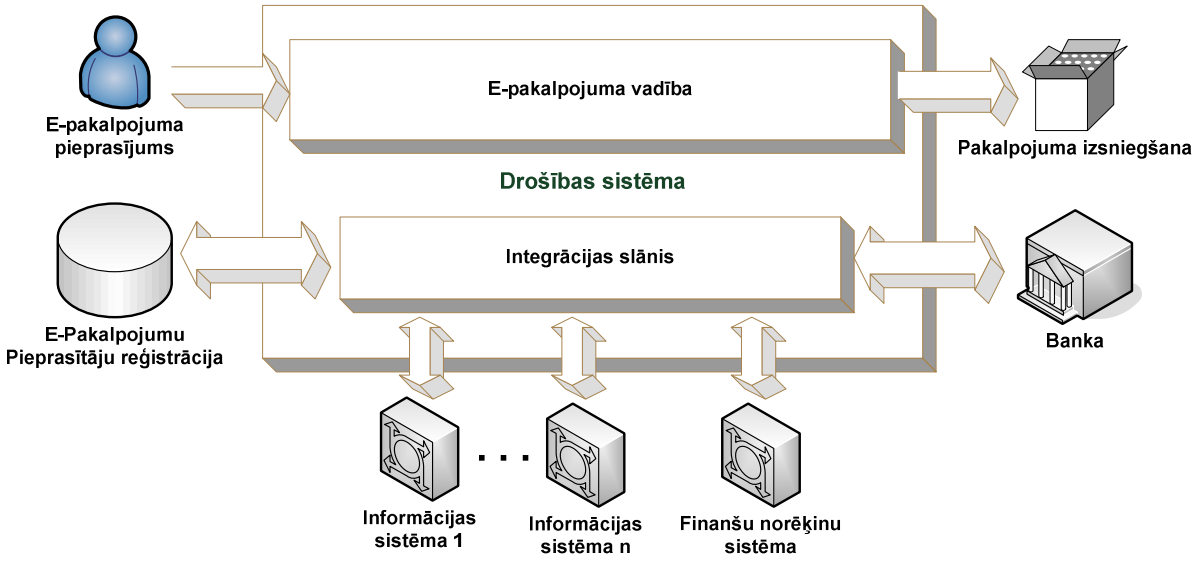
SOA pēc savas būtības nav nekāds jauninājums. Šāda veida arhitektūru ir iespējams izveidot arī tādās tehnoloģijās kā DCOM, CORBA un RMI. Šī raksta ietvaros ar servisiem tiek saprasti XML WEB servisi, kuri ir ieguvuši plašu popularitāti vienkāršības un platformu neatkarības pēc, kā arī tie ir specificēti un tiek attīstīti sadarbojoties dažādu tehnoloģiju izstrādātājiem, tāpēc tiem nākotnē ir paredzams plašs pielietojums[2].

E-pakalpojumu izveidē ir nepieciešams izmantot XML WEB servisus, lai samazinātu jaunu pakalpojumu izveides izmaksas, izmantojot esošus servisus. Šobrīd jau ir iespējams lietot tā saucamās otrās paaudzes WEB servisus, kuri sniedz plašas iespējas drošības sistēmas izveidē. Līdz ar to parādās problēmas, kuras ir saistītas ar esošu servisu izmantošanu jaunu pakalpojumu sintēzē, kā arī ar drošības līmeņa paaugstināšanu esošiem pakalpojumiem[3].

Pielietojot SOA e-pakalpojumu izveidē, ir jāņem vērā šīs arhitektūras specifika. Servisi ir vairāk vai mazāk neatkarīgi vienumi, pie kam vienā pakalpojumā var tikt izmantoti vairāki servisi. Tas nozīmē, ka drošība ir jāveido katram no servisiem. Pie kam ir jādomā par vienotu drošības sistēmas arhitektūras izveidi, ko būtu iespējams pielietot jebkuram e-pakalpojumam. Šādu e-pakalpojumu drošības sistēmas arhitektūras izveidi tad arī aplūkosim.

2. Drošības sistēmas arhitektūra

Drošības sistēmas arhitektūra ir viena no kopējās e-pakalpojumu arhitektūras sastāvdaļām, kuras vieta kopējā e-pakalpojuma arhitektūrā ir attēlota 2. attēlā.



2. attēls. E-pakalpojuma sistēmas arhitektūra.

Veidojot e-pakalpojumu drošības sistēmu, ir jāņem vērā vairāki nosacījumi, kuri obligāti ir jāizpilda. Katrs no nosacījumiem realizē kādu vispārēju drošības sistēmas arhitektūras daļu. Kā jau tika minēts, tad drošības jēdziens sastāv no trīs pamatlietām:

konfidencialitāte, integritāte un pieejamība. Aplūkosim nepieciešamās drošības sistēmas arhitektūras sastāvdaļas.

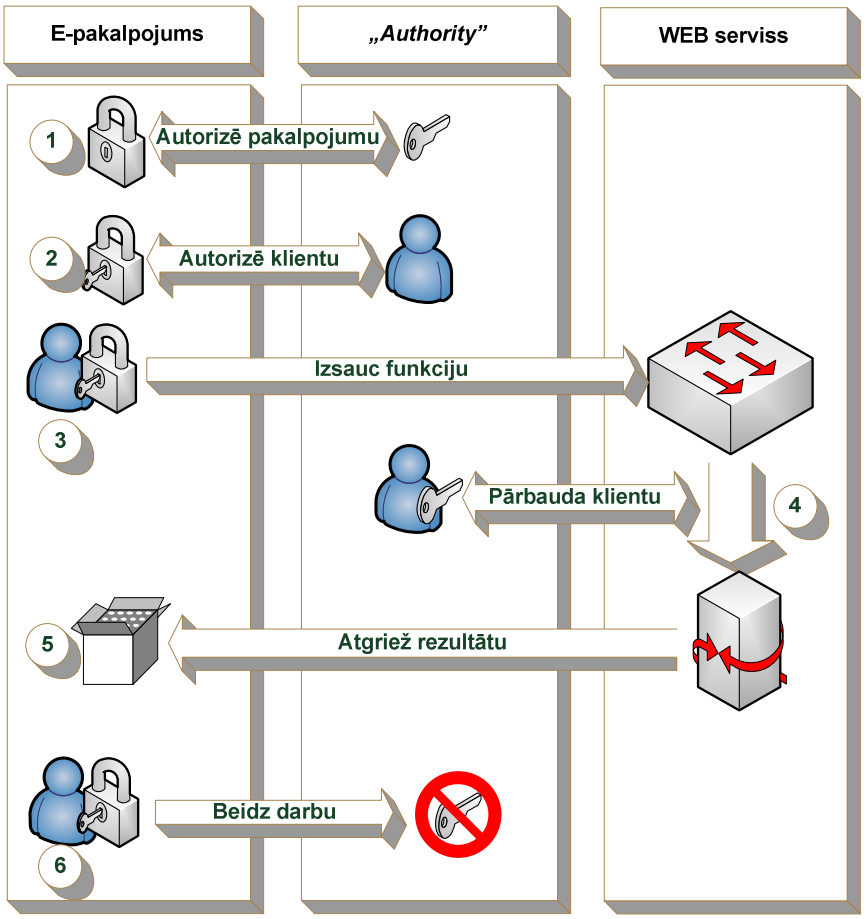
Konfidencialitāte galvenokārt saistīta ar lietotāju autentifikāciju, autorizāciju un datu šifrēšanu. Galvenās implementācijas īpatnības ir pakalpojumu lietotāju reģistra izveide un uzturēšana, jo kā jau tika minēts, tad valstī nav ieviests elektroniskais paraksts, kas dotu iespēju autentificēt jebkuru klientu. Kā otru īpatnību var minēt lietotāju sesiju un tiesību pārvaldību. Tas saistīts ar to, ka SOA e-pakalpojumu izveidē viens e-pakalpojums var izmantot vairākus servisus, kur katram no tiem ir realizētas kādas piekļuves tiesības. Vienu reizi pārbaudot klienta autentiskumu, tam ir jābūt iespējai piekļūt visiem nepieciešamajiem servisiem. Datu šifrēšanu var realizēt kanāla vai pieprasījumu/atbilžu līmenī. Uzmanību jāpievērš tam, ka realizējot šifrēšanu kanāla līmenī, datu pieprasījums var tikt nesankcionēti nolasīts kādā no tā pārraides starpposmiem, ja to maršrutē uz papildus apstrādi.

Integritāti galvenokārt nodrošina transakcijas un pieprasījumu/atbilžu parakstīšana. Jāpievērš uzmanība arī korektai kļūdu apstrādei un ievades un izvades datu atbilstībai iepriekš definētām datu struktūrām. Datu struktūru definīcijas, pēc iespējas, ir jālieto vienas un tās pašas, lai palielinātu izveidoto servisu atkārtotu izmantojamību. Tas savukārt ir saistīts ar datu struktūru reģistra izveidi. Pieprasījumu/atbilžu parakstīšana un validēšana ir jāsaista ar sesiju pārvaldību, lai nodrošinātu vienlaicīgi gan konfidencialitāti, gan integritāti.

Pieejamību drošības sistēmā galvenokārt nodrošina infrastruktūras arhitektūra, kā arī servisu modularitāte, kas samazina iespēju, ka kļūda vienā servisā izraisa visa pakalpojuma kļūdu. Tas nozīmē, ka, plānojot e – pakalpojumu, ir jāplāno arī tā izvietošana uz produkcijas vides serveriem. Projektējot servisus, ir jāatceras par e-pakalpojumu servisu izveides pamatprincipiem: minimāla servisu savstarpējā sasaiste un maksimāla servisu kohēzivitāte (saliedētība). Veidojot servisus pēc šādiem principiem, tiek palielināta to individuālā un līdz ar to arī visa e-pakalpojuma pieejamība[1].

3. Realizācija

Lai realizētu drošību e-pakalpojumos, ir izveidots drošības sistēmas modulis - *Authority*. Šis drošības modulis ir izveidots pietiekami universāls un to var izmantot ne tikai e-pakalpojumu realizācijā, bet arī jebkurā SOA uz XML WEB servisiem bāzētā aplikācijā. *Authority* moduļa darbības shēma ir attēlota 3. attēlā.



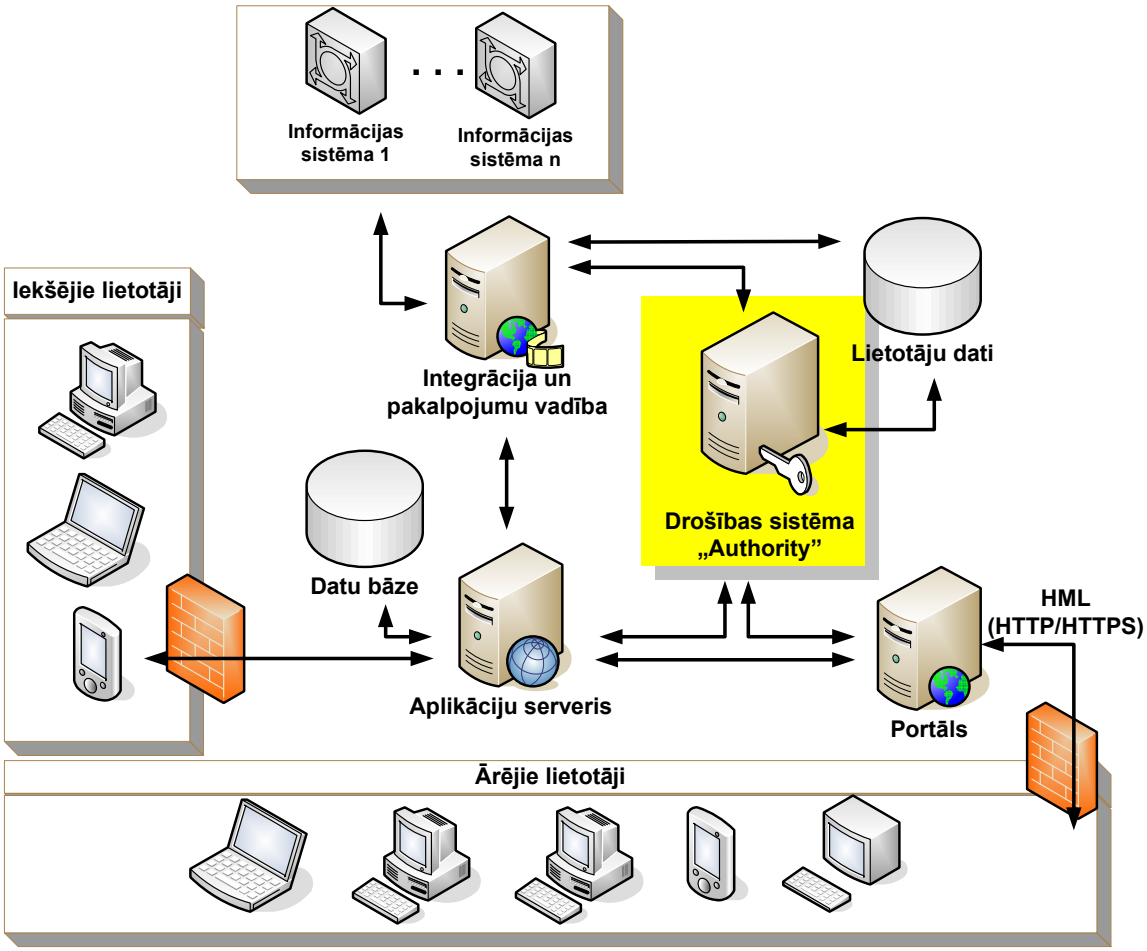
3. attēls. Drošības sistēmas darbības shēma.

Authority modulis nodrošina sekojošas drošības sistēmas prasības. Konfidencialitātes nodrošināšanai ir realizēta klientu autentifikācija un autorizācija, kas tiek balstīta uz „WS-Security" standartu[4]. Lielākā problēma ir klientu reģistra izveide. Lai nodrošinātu plašu e-pakalpojumu pielietojumu ir nepieciešams klientu reģistrs, kurā glabājas klientu autentifikācijas un autorizācijas dati. Šāds reģistrs ir vajadzīgs līdz brīdim, kamēr nav pilnībā ieviests elektroniskais paraksts un PKI. Par cik šāda vienota reģistra nav, tad ir izveidota iespēja lietot vairākus šādus reģistrus vienlaicīgi, ir tikai nepieciešams papildināt *Authority* moduli ar atbilstošā reģistra interfeisu. Modulī ir realizēti un apvienoti divi dažādi klientu autentifikācijas datu reģistri. Plašas iespējas šajā jomā paver banku klientu datu izmantošana autentifikācijai, jo lielākajai daļai valsts iedzīvotāju ir līgumi ar banku, un ir pieeja interneta bankām, kas ir droša autentifikācijas datu glabātuve. Problēma ir tāda, ka banku arī ir daudz, un tām katrai ir sava informācijas sistēma. Tas nozīmē, ka katrai no tām ir jāveido savs interfeiss ar *Authority* sistēmu. Autorizācijas nodrošināšanai modulis implementē tiesību pārvaldības mehānismu. Viena e-pakalpojuma realizācijai var tikt izmantoti dažādi servisi, tajā skaitā arī jau esoši servisi, kā arī servisi no dažādām funkcionālām sistēmām, tāpēc ir nepieciešama maksimāli pielāgojama tiesību pārvaldības sistēma. *Authority* modulis šo tiesību pielāgošanu realizē tiesību mantošanas ceļā. Ir iespējama tiesību mantošana no viena servisa uz otru pēc noteikta algoritma. Mantošanas algoritmu no servisa uz servisu ir iespējams konfigurēt. Modulis implementē arī pilnīgu klientu sesiju pārvaldību, neatkarīgi no tā, kurā no piesaistītajiem reģistriem glabājas klienta dati. Datu šifrēšanai var izmantot standarta kanāla šifrēšanas metodes, kā arī ir iespējams *Authority* modulī iestatīt noteiktu servisu pieprasījumu un atbilžu šifrēšanu.

Integritātes nodrošināšanai *Authority* modulī ir realizēta pieprasījumu/atbilžu parakstīšana un parakstu validēšana klienta sesijas ietvaros ar sesijas atribūtiem. Papildus ir nepieciešams realizēt kļūdu apstrādes moduli un datu struktūru reģistru. Datu struktūru

uzglabāšanai var izmantot dažādus standarta UDDI reģistru risinājumus. Transakciju risinājumiem XML WEB servisu gadījumā var pielietot „WS-Transaction" standartu[4]. Ja tiek izmantots cits risinājums servisu izveidei, tad ir jāpielieto risinājumam specifiski rīki un metodes.

Pieejamības uzlabošanai, kā jau tika minēts, ir nepieciešams izveidot atbilstošu infrastruktūru. *Authority* moduļa novietojums e-pakalpojumu sistēmas infrastruktūrā ir attēlots 4. attēlā.



4. attēls. Drošības sistēmas risinājums e-pakalpojumu sistēmā.

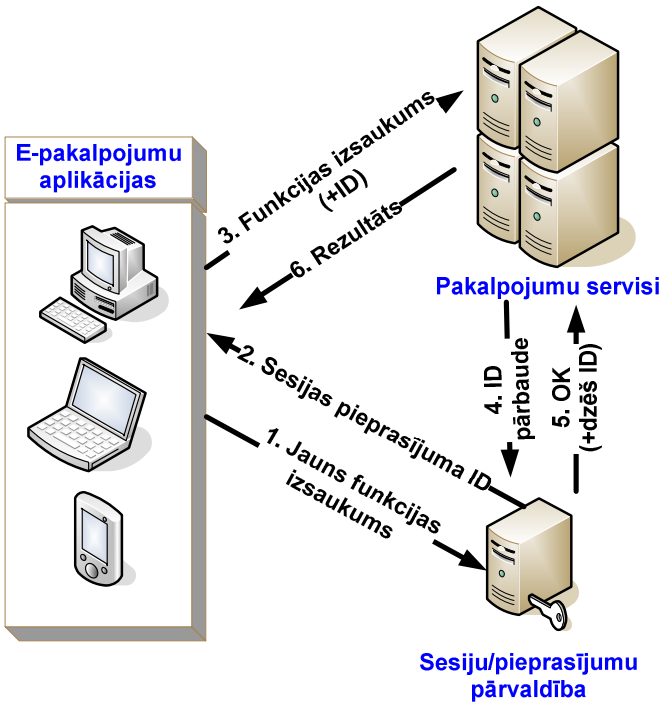
No pieejamības viedokļa pats *Authority* modulis ir „šaurā" vieta, jo, ja tas nav pieejams, tad nestrādās neviens e-pakalpojums. Šīs problēmas risinājums ir klientu sesiju datu pārvaldībai izmantot kādu datu bāzes pārvaldības sistēmu (DBPS) un serverus, uz kuriem atrodas gan *Authority* modulis, gan sesiju datu DBPS, klāsterizēt. Šāds risinājums atrisina sistēmas noslodzes problēmu, jo palielinoties e-pakalpojumu skaitam, ir prognozējama pietiekami liela noslodze *Authority* modulim.

Realizējot jaunus e-pakalpojumus un veidojot jaunus WEB servisus, ir ļoti ērti un lietderīgi pielietot augstāk minēto risinājumu. Problēmas ir ar drošības uzlabošanu esošos e-pakalpojumos, kā arī ar esošu WEB servisu izmantošanu e-pakalpojumos, kur tiek izmantots *Authority* modulis. Ja ir jāizmanto esoši WEB servisi, tad ir nepieciešams tos papildināt ar interfeisiem, kas realizē *Authority* sistēmas prasības.

Problēmas ir ar drošības uzlabošanu jau esošiem e-pakalpojumiem. Šāda risinājuma realizācija prasa pārāk lielus resursus esošas sistēmas pārveidošanai, un tas arī nav lietderīgi. Šādos gadījumos ir jāmeklē kompromiss starp prasībām un realizāciju, kas minimizē izmaiņu ieviešanas risku un izmaksas, un maksimizē vēlamo rezultātu.

Piemērs. Esošam maksas e-pakalpojumam ir nepieciešams uzlabot drošību, jo ir identificēti trūkumi esošajā risinājumā. E-pakalpojums ir izveidots, balstoties uz SOA arhitektūru. Tam ir klientu autentifikācija e-pakalpojuma interfeisā, bet servisu pieprasījumi

un atbildes netiek autentificētas un netiek arī šifrētas. Tas nozīmē, ka klients, zinot datu pieprasījumu formātu servisam, var iegūt datus par tiem nemaksājot, kā arī cits klients var noklausīties datus tīklā, kas tam nav paredzēti. Servisi šim pakalpojumam nav veidoti XML WEB servisu standartā. Integrēt šādā risinājumā *Authority* drošības moduli ir pārāk darbietilpīgi, kā arī riskanti, jo pakalpojums darbojas. Šajā gadījumā kompromisa variants ir veikt datu apmaiņas kanāla šifrēšanu un izveidot servisu autentifikāciju. Kanāla šifrēšanai vienkāršākais variants ir SSL pielietošana – servisu izsaukšana caur HTTPS protokolu. Servisu autentificēšanai ir nepieciešams izveidot lietotāju sesiju pārvaldības sistēmu kas attēlota 5.attēlā



5. attēls. Servisu autentifikācijas shēma.

4. Kopsavilkums

E-pakalpojuma drošības sistēmas izveides galvenais mērķis ir nodrošināt e-pakalpojuma sekmīgu izpildi visos izpildes soļos. Drošības sistēmas galvenie uzdevumi ir klientu autentifikācija un autorizācija, pakalpojuma integritāte un pieejamība. Šo uzdevumu izpildei ir nodefinēti nosacījumi, kurus ir nepieciešams implementēt drošības sistēmā.

Ir izveidots drošības sistēmas risinājums SOA bāzētai e-pakalpojumu sistēmai. Šis risinājums ir pielietojams jebkuram e-pakalpojumam un ir pietiekoši universāls. Ir atrisinātas autentifikācijas un autorizācijas problēmas, tajā skaitā arī tiesību pārvaldība SOA bāzētā e-pakalpojumu sistēmā. Kā arī ir atrisinātas dažas integrācijas un pieejamības problēmas. Papildus vēl ir jārisina sesiju pārvaldība, lai uzlabotu pieejamību, kā arī sistēmas ātrdarbība.

Piedāvātais risinājums ir viegli implementējams jaunizveidotos e-pakalpojumos, bet problēmas ir ar esošu e-pakalpojumu drošības uzlabošanu. Esošā risinājuma pielietošana tajos prasa pārāk lielus resursus. Tāpēc ir nepieciešams vienkāršots risinājums. Katram apskatāmajam gadījumam ir nepieciešama papildus analīze, bet drošības sistēmas idejas ir iespējams pielietot arī citos risinājumos, samazinot tā funkcionalitāti un izmainot tehnisko risinājumu.

5. Literatūra

1. The Open Web Applications Security Projects. A Guide to Building Secure Web Applications and Web Services. 2.0 Black Hat Edition 2005.07.27 – p. 293.

2. Thomas Erl. Service-Oriented Architecture. A Field Guide to Integrating XML and Web Services. Fourth Printing 2004. – p. 536.

3. E. Žeiris, M. Ziema. E-pakalpojumu izveides problēmas. Rīgas Tehniskās universitātes zinātniskie raksti. Datorzinātne. 5. sērija 19. sējums. Rīga 2004.g. 48 – 53 lpp.

4. http://www.oasis-open.org

Edzus Zeiris, M. Sc. Comp.
Riga Technical University
Faculty of Computer Science and Information Technology,
Institute of Computer Control, Automation and Computer Engineering
Address: Meža 1/3, 3rd floor. LV-1048, Riga, Latvia
E-Mail: edzus@zzdats.lv

Maris Ziema, Dr. Sc. Ing.
Riga Technical University
Faculty of Computer Science and Information Technology,
Institute of Computer Control, Automation and Computer Engineering
Address: Meža 1/3, 3rd floor. LV-1048, Riga, Latvia
E-Mail: maris@zzdats.lv

Žeiris E., Ziema M. Drošības risinājumi e – pakalpojumu sistēmās.
Rakstā tiek sniegts ieskats e-pakalpojumu drošības sistēmā un tās izveidē. Tiek vispārīgi aplūkotas e-pakalpojuma drošības prasības un to specifika, kas saistīta ar e-pakalpojuma izveides arhitektūru. Tiek definēta drošības sistēmas arhitektūra un tās vieta kopējā e-pakalpojumu sistēmas arhitektūrā. Detalizēti tiek aplūkots, ko nozīmē katrs no trīs galvenajiem drošības definīcijas punktiem e-pakalpojumu sistēmā un kā to nepieciešams realizēt. Ir aprakstīts konkrēts risinājums e-pakalpojuma drošības sistēmai un tā shematiska darbība. Dota atbilstība starp risinājuma un drošības prasību punktiem. Aplūkots arī, kas nepieciešams, lai pilnveidotu doto risinājumu, un tas apmierinātu visas izvirzītās prasības. Dotais risinājums ir pielietojams gan jaunām, gan esošām e-pakalpojumu sistēmām, bet par cik izmaiņas esošās sistēmās var prasīt lielus resursus, tad tiek piedāvāts risinājums esošu e-pakalpojumu sistēmu drošības uzlabošanai.

Zeiris E., Ziema M. Security Solutions for E – Service Systems.
Article gives introduction into e-services security system and shows its implementation. There are shown e-service security requirements and it's specific in general that is related to e-service development architecture. Security system architecture is defined and its place in general e-services architecture described. Each or three security definition points in e-services system content are described in details and defined possible implementation. Realization and its schematic workflow for e-service security system also are given. Relationship between realization and requirements are described. The required improvements for given realization are also described to implement all security architecture definition points. This realization is usable for new and also existing e-services systems. Implementation in existing system can take to many resources. For those cases there are given solution to improve security.

Жейрис Э., Зиема М. Решения безопасности в системах е-услуг
В статье рассматривается система безопасности е-услуг. Определяются требования по безопасности е-услуг и специфика, связанная с разработкой их архитектуры. Показана архитектура системы безопасности и её место в общей системе е-услуг. Подробно рассмотрено значение каждого из трёх основных составных частей безопасности и их реализация. Описано реальное решение для системы и схема его работы. Показаны отношения между реализацией системы и требованиям к ней, а также необходимые усовершенствования для полного соответствия реализации данным требованиям. Данное решение может быть использовано как новой, так и существующей системой е-услуг, однако так как внедрение решения в существующую систему может потребовать слишком много ресурсов, в статье предлагаются другие методы улучшения безопасности.