International Conference
FROM DELC TO VELSPACE
Plovdiv, 26–28 March 2014

ВЪТРЕШНА СИСТЕМА ЗА ОТОРИЗАЦИЯ И ПРИЛОЖЕНИЕТО Ѝ ЗА ЗАЩИТЕН ДОСТЪП ДО АКАДЕМИЧНИ ЕЛЕКТРОННИ УСЛУГИ

Емил Дойчев, Атанас Терзийски

Резюме. *В тази статия се описва създаването и развитието на оторизираща система (Фокус), разработвана за нуждите на Пловдивския университет през последните 10 години. Детайлно е представена архитектурата и основните предимства на третата версия (Фокус 3). Накратко са описани част от услугите, оторизирани от Фокус.*

Ключови думи: оторизация, обучение, сигурност, скалируемост, DeLC, Focus, e-learning

1. ВЪВЕДЕНИЕ

Фокус [1] е система за оторизация на потребители, разработена за нуждите на Пловдивския университет. Системата предоставя централизирано управление на потребители на различни видове информационни системи, работещи в компютърната мрежа на някои факултети в университета.

От създаването си Фокус търпи три основни промени:

1. През 2005 г. е разработен като система за оторизация, ориентирана към прокси услугата Squid [2], с цел въвеждане на квоти за интернет трафик, генериран от потребителите.
2. Във времето употребата на оторизиращата услуга на Фокус се утвърди и за други системи (виж параграф 3). Това наложи разработването на втора версия на Фокус с разширена поддръжка на потребителски роли и подобрен механизъм за регистрация на потребителите. Също така са добавени редица допълнителни модули:
   - модул за синхронизация на студентските профили с информационната система на учебното заведение (ИСУЗ) ;
   - поддържане на потребителите в LDAP сървър (OpenLDAP [3]);
   - модул за синхронизация с LDAP сървър.
3. Третата версия на системата се разработва със следните цели:
   - изолиране на Фокус от конкретната имплементация ИСУЗ;

- подобряване на възможностите за регистрация на студенти, информация, за които не се поддържа в ИСУЗ;
- семантично разширяване на поддържаните роли;
- изграждане на потребителски интерфейс, отговарящ на съвременните изисквания.

В годините системата се наложи като основно средство за оторизация на голяма част от услугите, предлагани в мрежата на университета. Понастоящем Фокус се характеризира със следните данни:

- в употреба от 2005 г.;
- създадени над 12000 уникални акаунти;
- над 6800 активни потребители;
- обслужва над 10 системи [4], работещи в компютърната мрежа на Пловдивския университет.

С развитието на системата Фокус става част от една по-обща архитектура на среда за предоставяне на електронни образователни услуги – DeLC [5].

2. ТРЕТА ВЕРСИЯ НА ФОКУС

Последната (трета) версия на Фокус се разработва в отговор на целите, изброени по-горе. За постигането им се използват различни съвременни технологии, чрез които се изгражда архитектурата на системата. Сред тях са:

- Grails [6] – framework за изграждане на приложението;
- Spring Security [7] за имплементация на механизмите са сигурност;
- Bootstrap [8], Bootswatch [9] и Font Awesome [10] за реализация на потребителския интерфейс.

Изолиране от ИСУЗ

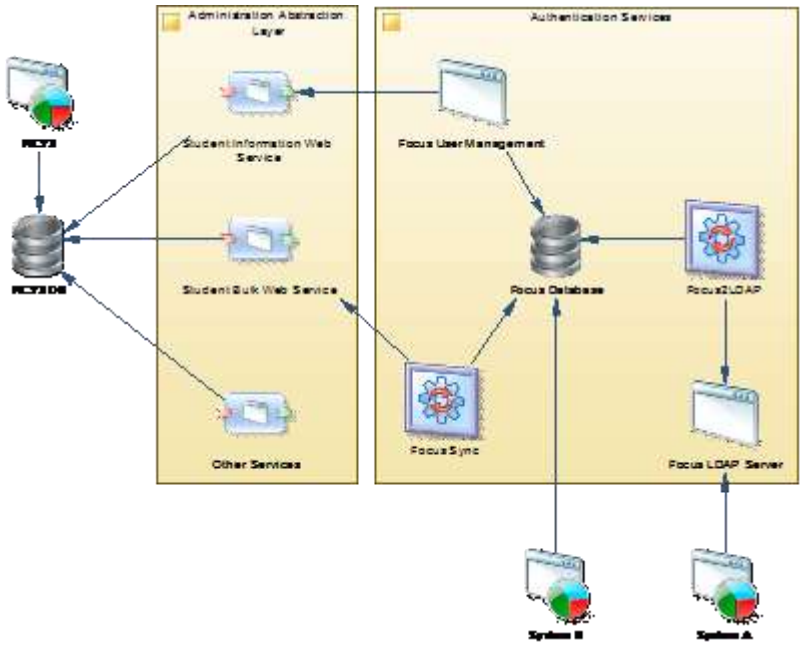
Изолирането на Фокус от ИСУЗ става чрез добавяне на междинен слой в комуникацията между ИСУЗ и Фокус. Този слой е изграден от web services (Фигура 1), които предоставят необходимите услуги за достъп до информацията, която се предоставя от ИСУЗ. Достъпът до този слой е защитен с необходимите механизми и комуникацията между Фокус и съответните web services е криптирана чрез SSL (OpenSSL [11]).

Подобряване на възможностите за регистрация

Съществен проблем на втората версия на Фокус е свързан с поддръжката (регистрация, удостоверяване и актуализиране на студентски права) на студентски акаунти, за които няма информация в ИСУЗ (например, студенти от филиали). Основно следствие е затрудненото и практически невъзможно предоставянето на услуги от системите, оторизирани от Фокус за тези студенти.

В третата версия на Фокус този проблем е решен по два начина. Първият механизъм е чрез добавяне на “web services”, чрез които може да се осъществи

достъп до база данни, различна от ИСУЗ, от където да се извлече информацията за тези студенти. Във Фокус 3 е реализирана логика, която позволява динамично да се конфигурират различни такива web services в зависимост от източниците на информация за студентите. Този механизъм е удобен когато има налична база данни, с информация за студентите.



Фигура 1. Архитектура на Фокус 3

Вторият начин е чрез новия механизъм за регистрация, при който не се използва автоматизирана валидация на акаунта. Вместо това в работния процес е включено участието на човек (в общия случай преподавател), който „активира“ определен набор от акаунти, след като лично потвърди достоверността на данните в тях. Този механизъм е предназначен за регистрация на малка група от хора, когато конфигурирането на отделен web service не е оправдано. При него се използва код-референция, който се въвежда като задължителен реквизит при регистрацията от страна на студента. Този код-референция се предоставя от преподавателя на групата студенти и той определя еднозначно както потребителя, който трябва да „активира“ акаунтите, така и специфични допълнителни атрибути на акаунтите като периода на валидност, факултета и специалността.

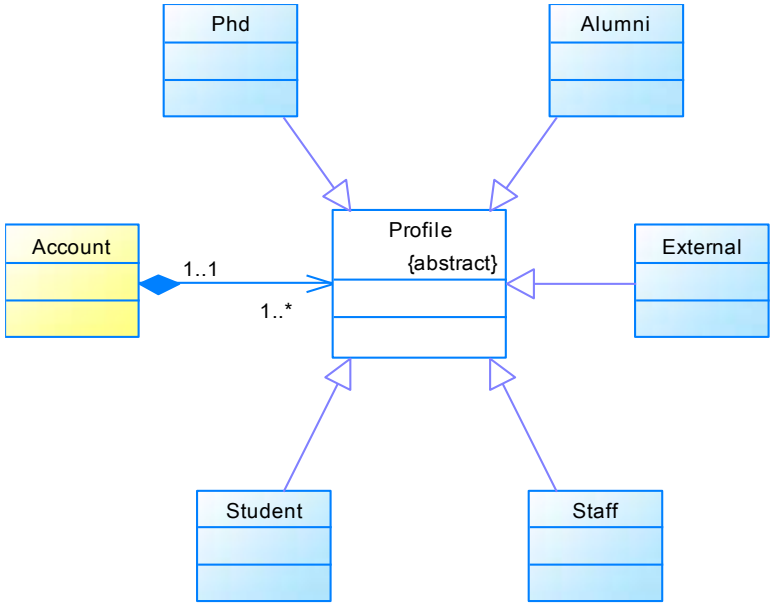
Разширяване на структурата на потребителския профил

Фокус поддържа няколко роли, които на абстрактно ниво определят ролята на потребителя в рамките на университета. В текущата версия те са: администратор, служител (в това число и преподаватели), студент и външен.

Един съществен проблем на втората версия е невъзможността един акаунт да притежава повече от една роля. Това косвено води до ограничения за създаване на повече от един студентски акаунт (напр. в случаите когато студента се обучава паралелно във втора специалност).

Във Фокус 3 отстраняването на този проблем се решава, чрез въвеждането понятията *акаунт* и *профил* (клас диаграмата на Фигура 2). Всеки потребител може да има само един *акаунт*, но към всеки акаунт могат да съществуват един или повече *профили*. Така семантиката на ролите се измества от ниво *акаунт* към ниво *профил*.

Видовете профили, които са дефинирани във Фокус 3 са: служител, студент, докторант, алумни и външен. При необходимост тази структура лесно може да бъде разширена допълнително с добавяне на нови видове профили.

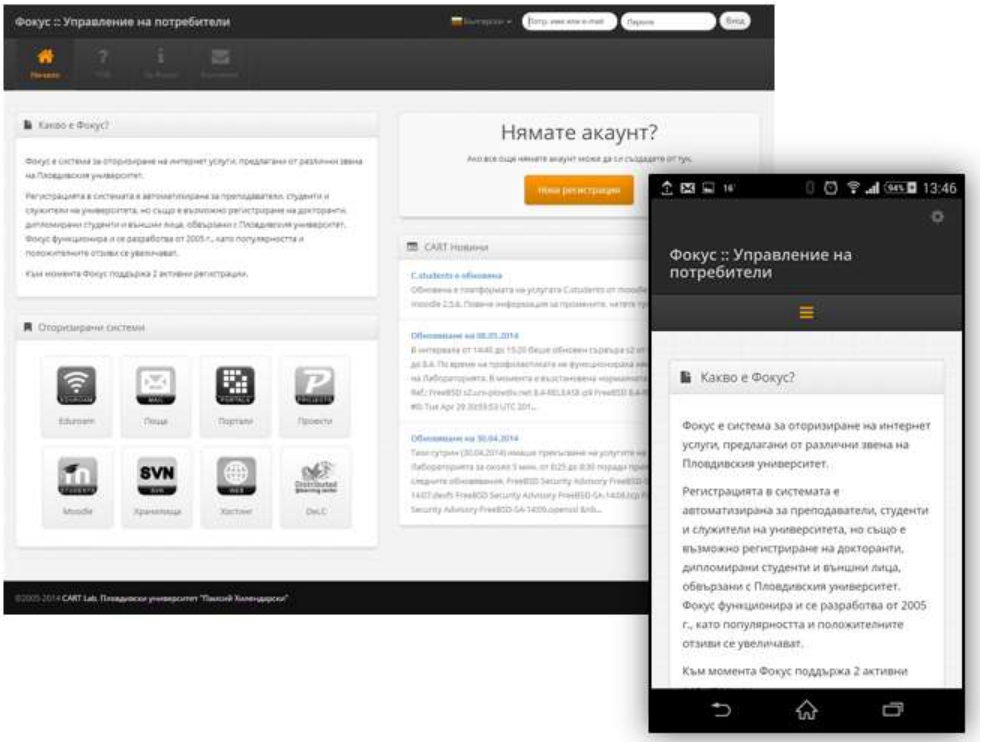


Фигура 2. Структура на потребителския профил

Съвременен потребителски интерфейс

Фокус е информационна система, в която над 85% от активните потребители са студенти. Всяка учебна година се създават над 2000 нови регистрации. В повечето случаи работата със системата се свежда до действията, свързани с поддържането на акаунт – регистрация, актуализация, смяна на парола и т.н. За тези дейности е удобно да се използват и мобилни устройства (таблет, смартфон и т.н.).

В тази връзка Фокус 3 следва тенденциите и потребителският му интерфейс (Фигура 3) е изцяло ориентиран към поддръжка на устройства с различни разделителни способности на дисплея.



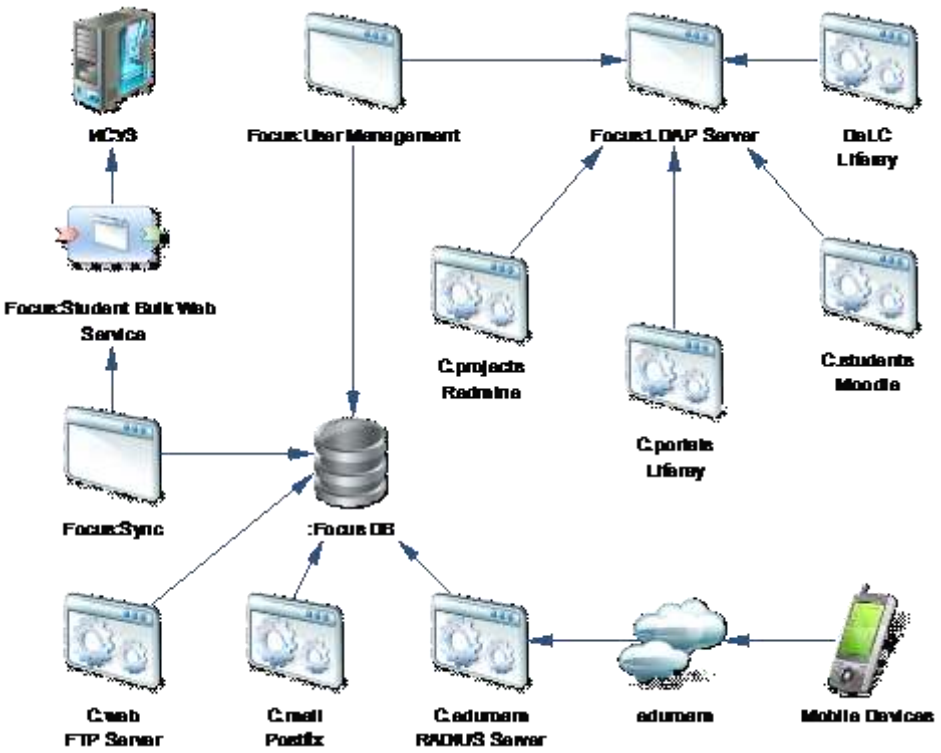
Фигура 3. Потребителски интерфейс

3. ПРИЛОЖЕНИЕ НА ФОКУС

В този параграф с кратко описание и метод на оторизация са представени някои от най-популярните услуги, ползващи оторизация чрез Фокус. Списък [4] на по-голямата част от Фокус оторизираните услуги може да бъде видян на сайта на Лабораторията за компютърно подпомагане на обучението и научните изследвания [12]. На фигура 4 е показана част от инфраструктурата, изградена с помощта на Фокус. Информацията за услугите е актуална към март 2014 г.

- C.eduroam [13] е вътрешно-университетска услуга, базирана на eduroam (EDUcation ROAMing) [14]. По същество това е услуга, позволяваща на членуващите академични институции да предоставят на потребителите си надежден безжичен достъп до интернет в коя да е eduroam членуваща институция по света. Това е възможно чрез редица технологии [15] и споразумения. Крайната цел е изграждане на роуминг инфраструктура, така че крайните потребители да имат достъп до интернет с всяко преносимо устройство (лаптоп, таблет, смартфон и т.н.). Имплементацията на C.eduroam в Пловдивския университет е базирана на FreeRADIUS [16], като Фокус оторизацията се извършва чрез

директни заявки към базата данни. Отчетената средна активност е от няколко стотин успешни дневни оторизации на Фокус потребители.



Фигура 4. Инфраструктура

- C.mail е комплексна услуга за електронна поща, базирана на Roundcube [17], Postfix [18] и Dovecot [19]. Оторизацията се извършва чрез директни заявки към "view" на Фокус базата данни. Активността на 64 потребителя е няколко стотин писма на ден.
- C.portals се оторизира от Фокус чрез LDAP и представлява услуга за разработване на динамични сайтове, базирани на порталната платформа Liferay [20]. Над 200 потребителя използват услугата. Създадени са близо 30 сайта.
- C.projects се базира на Redmine [21] и представлява услуга за управление на проекти. Около 200 потребителя работят по 50 проекта. Оторизацията от Фокус е чрез LDAP.
- C.students е услуга, базирана на Moodle [22] и се ползва за електронни и дистанционни курсове и учебни материали. Системата поддържа над 5700 потребителя и 250 курса. Оторизацията от Фокус е чрез LDAP.
- C.web е класическа услуга за хостинг на интернет страници чрез FTP достъп, реализиран с PureFTPd [23]. Услугата поддържа близо 800 страници на потребители.

- DeLC (Distributed eLearning Center) [24, 25] е портал, ориентиран към предоставянето на електронни услуги за обучение. Порталът е базиран на Liferay и се оторизира от Фокус чрез LDAP.

ЛИТЕРАТУРА

[1] Focus User Management, http://focus.uni-plovdiv.net, посетен на 19.05.2014.
[2] Squid: Optimising Web Delivery, http://www.squid-cache.org, посетен на 21.05.2014
[3] OpenLDAP, Main Page, http://www.openldap.org/, посетен на 21.05.2014
[4] CART Lab., услуги, http://cart.uni-plovdiv.net/services, посетен на 21.05.2014
[5] Дойчев, Е., „*Среда за електронни образователни услуги*“, дисертация, Пловдивски университет „П. Хилендарски“, 2013 г.
[6] Grails Franework, https://grails.org/, посетен на 31.03.2014
[7] Spring Security, http://projects.spring.io/spring-security/, посетен на 31.03.2014
[8] Bootstrap, http://getbootstrap.com/, посетен на 31.03.2014
[9] Bootswatch, http://bootswatch.com/, посетен на 31.03.2014
[10] Font Awesome, the iconic font and CSS framework, http://fontawesome.io/, посетен на 31.03.2014
[11] OpenSSL: The Open Source toolkit for SSL/TLS, http://www.openssl.org, посетен на 21.05.2014
[12] Лаборатория за компютърно подпомагане на обучението и научните изследвания, http://cart.uni-plovdiv.net, посетен на 21.05.2014.
[13] C.eduroam, http://eduroam.uni-plovdiv.bg, посетен на 21.05.2014
[14] Eduroam, http://eduroam.org, посетен на 21.05.2014
[15] The eduroam architecture for network roaming, http://tools.ietf.org/html/draft-wierenga-ietf-eduroam, посетен на 21.05.2014
[16] FreeRADIUS: The world's most popular RADIUS Server, http://freeradius.org, посетен на 21.05.2014
[17] Roundcube – Free and Open Source Webmail Software, http://roundcube.net, посетен на 21.05.2014
[18] The Postfix Home Page, http://www.postfix.org, посетен на 21.05.2014
[19] Dovecot, http://www.dovecot.org, посетен на 21.05.2014
[20] Liferay – Enterprise open source portal and collaboration software, http://www.liferay.com, посетен на 21.05.2014
[21] Redmine, http://www.redmine.org, посетен на 21.05.2014
[22] Moodle – Open-source learning platform, http://moodle.org, посетен на 21.05.2014
[23] Pure-FTPd, http://www.pureftpd.org, посетен на 21.05.2014

[24] Stoyanov, S., I. Popchev, E. Doychev, D. Mitev, V. Valkanov, A. Stoyanova-Doycheva, V. Valkanova and I. Minov, DeLC Educational Portal, Cybernetics and Information Technologies (CIT), Vol. 10, No. 3., *Bulgarian Academy of Sciences*, 2010, 49–69.
[25] Stoyanov, S. V. Valkanova, G. Cholakov and M. Sandalski, Education Portal for Reactive and Proactive Service Provision, *COGNITIVE 2011: The Third International Conference on Advanced Cognitive Technologies and Applications*, 25–30 September, 2011, Rome, 99–103, ISBN: 978-1-61208-155-7.

Emil Doychev
University of Plovdiv
Faculty of Mathematics and Informatics
236 Bulgaria Blvd, 4003 Plovdiv
e.doychev@uni-plovdiv.net

Atanas Terziyski
University of Plovdiv
Faculty of Chemistry
24 Tzar Asen Str., 4000 Plovdiv
atanas@uni-plovdiv.net

AN INTERNAL AUTHORIZATION SYSTEM AND ITS APPLICATION FOR A TRUSTED ACCESS TO ACADEMIC SERVICES

Emil Doychev, Atanas Terziyski

Abstract. *This paper introduces the creation and development of an authorization system (Focus), which has been developing for University of Plovdiv in the past 10 years. The architecture and main advantages of the system (Focus 3) are described in details. Descriptions of several applications that are authorized by Focus are also included.*