ПРАВИЛНИК О ОРГАНИЗАЦИОНИМ И ТЕХНИЧКИМ МЕРАМА ЗА УНАПРЕЂЕЊЕ ИНТЕРНОГ ИНФОРМИСАЊА

Донет на седници Савета Универзитета у Новом Саду одржаној 9.6.2016. године
Ступио на снагу: 30.6.2016.

Број: 01-74/5-4
Датум: 9.6.2016. године

На основу члана 70 став 1 тачка 13 Статута Универзитета у Новом Саду (Савет Универзитета 28. децембра 2010. године, измене и допуне 23. марта 2012. године, 11. октобра 2012. године, 26. фебруара 2013. године, 15. новембра 2013. године, 30. маја 2014. године, 04. јуна 2015. године и 29. јануара 2016. године), на предлог Сената Универзитета у Новом Саду од 02. јуна 2016. године, Савет Универзитета на 5. седници одржаној 09. јуна 2016. године, доноси

ПРАВИЛНИК О ОРГАНИЗАЦИОНИМ И ТЕХНИЧКИМ МЕРАМА ЗА УНАПРЕЂЕЊЕ ИНТЕРНОГ ИНФОРМИСАЊА

УВОДНЕ ОДРЕДБЕ

Предмет уређивања

Члан 1

Овим Правилником утврђују се организационе и техничке мере које треба да омогуће унапређење квалитета непосредног интерног информисања и квалитета коришћења информационих ресурса.

Потпуна имплементација организационих и техничких мера из овог правилника обезбеђује могућност за интеграцију база идентитета са циљем интеграције информационо технолошких (у даљем тексту: ИТ) сервиса на нивоу Универзитета.

Основни појмови

Члан 2

Интерно информисање посредством академске мреже Универзитета у Новом Саду (у даљем тексту: Универзитет) изводи се посредним и непосредним методама информисања. За посредну методу информисања користи се објављивање обавештења на веб презентацијама чланица Универзитета. За непосредну методу информисања користи се директно прослеђивање обавештења корисницима академске мреже, запосленим и студентима, електронском поштом на њихове адресе сервиса електронске поште чланица Универзитета.

Информационе технологије, у области информисања, фаворизују непосредне методе информисања. Поред сервиса електронске поште, за непосредне методе информисања користе се сервиси за размену порука на друштвеним мрежама и другим *cloud* платформама. Непосредне методе информисања претпостављају директно обраћање кориснику преко података из његовог дигиталног идентитета.

Дигитални идентитет корисника је скуп података који кориснику омогућава коришћење информационих сервиса који су подешени да на основу тих података омогуће приступ и коришћење одређених информационих ресурса. Индивидуализован приступ и садржај су код ове класе сервиса неопходни да би се обезбедила приватност комуникације (као што је случај код електронске поште), ауторизација на основу припадности одређеној категорији, као и административно и безбедносно праћење коришћења ресурса.

Одржавање дигиталних идентитета је административно захтевна активност, уколико се инсистира на ажурности и потпуности података који се складиште везано за кориснике.

Ажурност је неопходна да би се избегле ситуације које би могле да деградирају неки сервис како за појединачног корисника, тако и за све кориснике; примера ради, злоупотреба сервиса, присвајање идентитета и безбедносни пропусти.

Дигитални идентитети се складиште у базама идентитета. Базе идентитета се називају и именици идентитета.

Са техничке стране, системи за складиштење идентитета по правилу нису веома захтевни по питању рачунарских ресурса, нарочито у случају мањих скупова података (реда неколико стотина.) Технички проблеми који захтевају интензивније ангажовање и већу стручност најпре се односе на потребе интеграције базе идентитета са спољашњим сервисима.

Појединачни корисник може припадати различитим базама (именицима) дигиталних идентитета. Обједињавање тих база има смисла за случајеве употребе који се могу подвести под исту општу класу по неком критеријуму, и не мора се инсистирати на потпуном елиминисању свих различитости; са становишта безбедности, чак је и пожељно да различите класе коришћења (примера ради: пословна и приватна, у најгрубљој подели) имају дисјунктне параметре и начин одржавања. Класа случајева употребе на Универзитету може се оквирно назвати пословном употребом мрежних сервиса у академском окружењу ван непосредне локалне повезаности.

На Универзитету сви запослени и студенти везани за појединачну институцију имају право коришћења мрежних сервиса који ће користити претпостављену базу дигиталних идентитета. Ако постоји локална политика која ограничава приступ овим сервисима, она се примењује после општих правила за утврђивање идентитета корисника, и спада у надлежност појединачне чланице Универзитета.

Дигитални идентитети корисника, њихове базе и интегрисаност база идентитета са спољашњим сервисима кључни су елементи који утичу на квалитет непосредног информисања и квалитет коришћења информационих ресурса Универзитета.

Под појмом чланица Универзитета, у смислу овог Правилника, сматрају се факултети, институти и друге организационе јединице у саставу Универзитета у Новом Саду.

Тренутно стање

Члан 3

Анализа постојећег стања база дигиталних идентитета институција Универзитета изведена је тако да прикаже специфичности стања Универзитета. Када се у најширем смислу обухвати термин база идентитета може се закључити да за једну институцију постоји више база идентитета намењених различитим употребама. У случају посматрања база идентитета које се односе на сервисе академске мреже Универзитета добијају се резултати који у даљим активностима нуде решење за интеграцију података о идентитетима и њиховим управљањем. Специфичност стања Универзитета огледа се кроз следеће:

• Постоји централна база идентитета на које добровољно имају право сви запослени и студенти Универзитета.

• Централна база идентитета је главна база за неке од институција Универзитета.

• Централна база идентитета садржи идентитете корисника који имају и своје идентитете у базама на матичним институцијама.

• Централна база идентитета је интегрисана са више спољашњих сервиса: mail@uns; webmail@uns; vpn@uns; dial-in@uns; EduRoam@uns; cloud@uns; портал стручних већа Сената Универзитета; портал Сената Универзитета; портал Савета Универзитета; систем за резервацију простора Универзитета;

• Чланице Универзитета поседују своје базе идентитета.

• У већини случајева појединачни сервис користи изоловану, за своје потребе, креирану базу идентитета.

• Изузетак је база идентитета на Природно-математичком факултету која је интегрисана са више спољашњих сервиса: EduRoam@uns; студентски портал ПМФ-а; webmail@PMF; Moodle e-learnig ПМФ-а; информациони систем студентске службе ПМФ-а.

Мере за унапређење

Члан 4

Из горе наведеног, а у циљу унапређења квалитета интерног информисања и квалитета коришћења информационих ресурса закључује се да је неопходно извршити интеграцију база дигиталних идентитета што ће омогућити и интеграцију ИТ сервиса на нивоу Универзитета. За ове потребе одређују се организационе и техничке мере прописане правилником.

Очекивани ефекти

Члан 5

Организационе мере обезбеђују формално дефинисање носилаца одговорности и носилаца права за приступ подацима из база идентитета и њихову употребу у циљу непосредног информисања.

Техничке мере обезбеђују:

• извршиоце непосредног информисања и њихове улоге;

• непосредне извршиоце претраживања база идентитета;

• архитектуру базе идентитета и протокол за приступ бази идентитета који омогућавају интеграцију база идентитета на нивоу Универзитета и интеграцију са спољашњим сервисима;

• стандарде за формат записа у базама идентитета који омогућавају интеграцију база идентитета на нивоу Универзитета и интеграцију са спољашњим сервисима;

• стандарде за администрацију записа у базама идентитета који обезбеђује висок ниво ажурности и тачности записа;

• дефинисане архитектуре и дефинисани стандарди обезбеђују повезивање информационих система студентских служби, кадровских служби и других информационих система званичних регистара на Универзитету са сервисима непосредног информисања и другим ИТ сервисима свих чланица Универзитета, као и са спољашњим сервисима.;

• стандарде за техничку имплементацију и начине превазилажења инфраструктурних и кадровских ограничења у појединачним институцијама за техничку имплементацију.

ОРГАНИЗАЦИОНЕ МЕРЕ

Члан 6

На нивоу Универзитета дефинише се интеграциони дигитални идентитет који је ауторизован за:

• техничко прослеђивање обавештења, непосредним методама информисања, свим корисницима који су дефинисани у базама дигиталних идентитета чланица Универзитета и/или су дефинисани у централној бази дигиталних идентитета Универзитета;

• претраживање свих база дигиталних идентитета које ће се креирати у складу са техничким мерама из овог правилника;

Ректор Универзитета решењем дефинише техничко тело које је одговорно за све аспекте рада са интеграционим дигиталним идентитетом.

Члан 7

На нивоу чланице Универзитета дефинише се институционални дигитални идентитет који је ауторизован за:

• техничко прослеђивање обавештења, непосредним методама информисања, свим корисницима који су дефинисани у базама дигиталних идентитета чланице Универзитета;

• претраживање свих база дигиталних идентитета чланице Универзитета, а које ће се креирати у складу са техничким мерама из овог правилника;

Декан/директор чланице Универзитета решењем дефинише техничко тело које је одговорно за све аспекте рада са институционалним дигиталним идентитетом.

ТЕХНИЧКЕ МЕРЕ

Члан 8

До реализације потпуне интеграције база дигиталних идентитета на Универзитету, обавезују се сва техничка тела одговорна за рад са институционалним дигиталним идентитетима да примљена обавештења, чији пошиљалац је аутентификовани интеграциони дигитални идентитет, проследи непосредним методама информисања, свим корисницима који су дефинисани у базама дигиталних идентитета чланице Универзитета.

ДИГИТАЛНИ ИДЕНТИТЕТ

Члан 9

У општем случају, сваки дигитални идентитет одговара једном запису у бази података која га садржи. Запис се посматра као скуп атрибута, од којих сваки има своје име и скуп вредности. Иако се технологија за имплементацију базе идентитета не мора стриктно ограничити на одређену категорију, употребљена терминологија, карактеристике приступа бази и развијеност технолошког окружења упућују на јасну препоруку да база буде хијерархијска, а обавезу да буде доступна преко LDAP протокола, на начин описан у одељку „ТЕХНИЧКА ИМПЛЕМЕНТАЦИЈА“ у прилогу овог правилника. Програмски пакет OpenLDAP је референтна имплементација са добром подршком под отвореним серверским системима и његово коришћење се препоручује.

УПРАВЉАЊЕ ИДЕНТИТЕТИМА

Члан 10

Чланица Универзитета мора имплементирати све административне и техничке поступке и ресурсе потребне за реализацију базе дигиталних идентитета. (Ово не прејудицира детаље техничког решења, које може бити локално, удаљено, или комбинација та два.) За административне поступке треба се у потпуности ослонити на већ постојеће процедуре дефинисане унутар институције, а реализоване унутар кадровске, односно студентске службе институције. ИТ служба чланице Универзитета треба да омогући техничке услове за реализацију базе дигиталних идентитета. Ово подразумева локално управљиву и доступну базу идентитета над којом се могу обављати све операције које административни поступак захтева. Овај документ не може исцрпно да наведе све техничке варијанте које би омогућиле

имплементацију овакве базе, па ће у наставку бити дат кратак преглед техничких параметара локалне инсталације која овакву базу обезбеђује. Детаљне техничке смернице за управљање идентитетима дате су у прилогу овог правилника и чине његов саставни део (Прилог I).

ТЕХНИЧКА ИМПЛЕМЕНТАЦИЈА

Члан 11

С обзиром на карактеристике приступа бази дигиталних идентитета, сматраћемо да ће чланица Универзитета следити препоруке из горњег одељка који описује рад са базом на општи начин, тј. да ће се користити софтверски пакет OpenLDAP. Детаљне техничке смернице за техничку имплементацију дате су у Прилогу I.

ПРИМЕР ИМПЛЕМЕНТАЦИЈЕ

Члан 12

Због недостатка техничких ресурса чланице Универзитета могуће је значајан део поступака одржавања дигиталних идентитета, пренети одговарајућој служби друге чланице Универзитета, под претпоставком да таква служба постоји и технички је оспособљена за предвиђене послове. Оваква стратегија може значајно да смањи административно и техничко оптерећење чланице Универзитета која је примени.

Члан 13

Чланице Универзитета, као и институције територијално, организационо и функционално везане за Универзитет имају могућност делегирања административних и техничких послова везаних за базе дигиталних идентитета одговарајућој служби Универзитета (ЦИТ-УНС).

Члан 14

Универзитетска служба је дужна да обезбеди техничке услове за регистрацију корисника локалној служби чланице Универзитета која је одговорна за проверу идентитета корисника, евентуално слагање с локалном политиком права на добијање идентитета и валидност изабраних предлога корисничких имена и лозинки.

Након регистрације, даљи рад с корисницима може се препустити универзитетској служби.

Промена основних података о кориснику, као што су име или презиме, може се обавити слањем обавештења о промени од стране локалне службе чланице Универзитета универзитетској служби или на захтев корисника дигиталног идентитета.

Члан 15

Овај Правилник ступа на снагу осмог дана од дана објављивања на интернет страници Универзитета.

ПРЕДСЕДНИК САВЕТА

Академик проф. др Ненад Вуњак

ПРИЛОГ I

ТЕХНИЧКО УПУТСТВО

ДИГИТАЛНИ ИДЕНТИТЕТ

У LDAP окружењу, структура записа је у складу са шемом, која представља скуп дефиниција појединачних атрибута и правила за њихово коришћење и груписање. Сваки запис мора припадати једној структурној класи, која одређује основну структуру записа, у виду списка обавезних и необавезних атрибута. Скупови додатних атрибута дефинишу се у помоћним класама. Како је управљање идентитетима од почетка препознато као важан случај коришћења LDAP-а, већ дуго постоје стандардизоване класе за смештај података о идентитету. Једна таква класа је **`inetOrgPerson`**, која је добра полазна основа за идентитет особа, због чега се она препоручује.

Класа **`inetOrgPerson`** као обавезне атрибуте захтева **`cn`** (commonName, уобичајено се поставља на пуно име особе) и **`sn`** (surname, само презиме; ако структура имена не познаје појам презимена, понавља се пуно име), и допушта **`uid`** (алфанумерички идентификатор корисника, јединствен у оквиру институције), као и **`userPassword`** (лозинка за приступ.) У пракси је овај минимални скуп атрибута довољан за већину употреба, нарочито у оквиру институција без разуђене организационе структуре, где је контекст идентитета ограничен величином организације. Препоручује се да наведена четири атрибута буду формално проглашена за обавезне помоћу механизма као што је LDAP правило садржаја (DIT Content Rule), како би се избегло креирање непотпуних записа. У одељку „ТЕХНИЧКА ИМПЛЕ¬МЕНТАЦИЈА“ наведен је скуп обавезних атрибута, као и обавезна функционалност приликом претра¬живања записа, са препорукама организације записа ради лакшег испуњења ових обавеза.

Пошто је корисничко име, одређено атрибутом **`uid,`** основни параметар за идентификацију, пожељно је да то име има значење за особу које га користи. Зато се препоручује да то име не буде механички генерисано, већ да се кориснику да могућност избора бар две варијанте, од којих би се свака после прве користила ако све претходне доводе до колизије са већ регистрованим именима. Да избор имена не би био сасвим непредвидљив, препоручује се увођење минималног скупа синтаксних ограничења, нпр. минималне дужине од три знака, обавезе да први знак буде алфабетски, и редуковање скупа знакова на слова енглеске абецеде, цифара, и подвлаке.

Приступна лозинка би требало да буде позната само кориснику, и да механизам за њену промену може да диктира параметре минималне сложености, како би се избегло њено једноставно погађање и злоупотреба идентитета за лажно представљање и присвајање ресурса. Препоручује се да за лозинку постоји минимална дужина (6-8 знакова), обавезност постојања бар једног великог слова, цифре и знака интерпункције, као и провера да ли изабрана лозинка може да се погоди претрагом речника или тривијалним трансформацијама корисничког или пуног имена. Такође се препоручује да трајање лозинке буде ограничено роком који неће представљати непогодност у коришћењу идентитета, а ипак ће моћи да спречи потенцијалну злоупотребу запуштених идентитета; могућ период је шест месеци од датума последње промене

Додатни атрибути обогаћују податке о идентитету и омогућавају имплементацију богатијег скупа сервиса, као и лакшу идентификацију корисника у одређеним сценаријима. Ове предности проширења основног скупа атрибута не треба да поставе у други план правило да неажурност података ограничава њихову употребљивост једнако као и мали расположив скуп. Препоручује се записивање само оних атрибута у чију поузданост и ажурност нема основане сумње; ово је утолико битније ако се одређени атрибути прогласе за обавезне.

Један од могућих извора додатних атрибута су класе развијене за потребе академских средина, као што су **eduPerson и eduOrg**. Ове класе су дефинисане као помоћне, тако да се могу лако додати основном запису. AMPEC је развио шему **eduRS**, чије су класе изведене из ове две и могу се користити као основа за бележење идентитета, с том разликом што је број обавезних атрибута већи, а класе **rsEduPerson и rsEduOrganization** дефинисане као структурне у садашњој дефиницији шеме, што би подразумевало релативно ригидну структуру именика; очекује се да ће ове шеме бити измењене тако што ће поменуте класе постати помоћне, а атрибути проглашени необавезним, у ком случају нема препреке за њихово коришћење у препорученој организацији именика.

УПРАВЉАЊЕ ИДЕНТИТЕТИМА

Регистрација корисника

За регистрацију корисника и доделу креденцијала, институција мора имати процедуру којом проверава идентитет корисника и евентуално слагање с локалном политиком права на добијање идентитета. Препорука је да се додела креденцијала кориснику обавља искључиво на захтев корисника. На овај начин се смањује могућност злоупотребе дигиталног идентитета и повећава сигурност сервиса чије коришћење зависи од употребе дигиталних идентитета.

Промена корисничких параметара

Промена основних података о кориснику, као што су име или презиме, може се обавити на захтев корисника или на захтев службе одговорне за администрацију корисника. Преоручује се да корисничка имена буду фиксна и перманентна, а лозинке временски ограниченог трајања.

Конструкција јединственог идентификатора

Ради интеграције институције са спољашњим сервисима коришћењем постојеће базе дигиталних идентитета, потребно дефинисати јединствени идентификатор, који би недвосмислено представљао све идентитете у оквиру институције (на најгрубљем нивоу грануларности.) Уколико постоји потреба за финијом расподелом, може се дефинисати више идентификатора. Одржавање мапирања ових идентификатора је одговорност службе за администрацију корисника.Промена основних података о кориснику, као што су име или презиме, може се обавити на захтев корисника или на захтев службе одговорне за администрацију корисника. Препоручује се да корисничка имена буду фиксна и перманентна, а лозинке временски ограниченог трајања.

Укидање/гашење корисничког идентитета

Укидање корисничког идентитета спада у исту врсту администриративних процедура као и било која промена корисничких параметара. Препорука је да се подаци не биришу из базе дигиталних идентита већ да се онемогући приступ сервисима.

ТЕХНИЧКА ИМПЛЕМЕНТАЦИЈА

У једном успостављеном систему, провера идентитета и права приступа је критичан сервис, тако да његова доступност мора бити на високом нивоу. Препоручује се да LDAP сервис буде реплициран у master/slave или multimaster топологији, као и да постоји систем за активно/пасивно или активно/активно балансирање и преузимање сервиса у случају отказа. Решења за балансирање и преузимање су многобројна и не може се инсистирати на неком одређеном, сем опште напомене да за је мање инсталације, реда стотина корисника, софтверска имплементација довољна да обезбеди солидну доступност.

Компатибилност са спољашњим сервисима може се постићи посебним мапирањем и надоградњом атрибута; у OpenLDAP серверу ово се постиже rwm и translucent модулима. Имплементација спреге са **RADIUS** сервером за проверу идентитета мора се узети у обзир уколико институција жели самостално да се укључи у eduroam заједницу. Препоруке за имплементацију eduroam сервиса су посебно описане у eduroam документацији (https://www.eduroam.org/index.php?p=docs), која ће овде бити само референцирана.

Обавезни начини приступа бази идентитета

База идентитета мора бити доступна преко верзије 3 (три) LDAP протокола. Приступна тачка мора бити заштићена помоћу TLS протокола, било посредством **ldaps** транспорта (што се препоручује), било посредством комбинације **ldap** транспорта и **StartTLS** операције. Приступ се мора ограничити на ауторизовани скуп корисника, који се морају пријавити пре коришћења операција претраге.

Обавезни и препоручени атрибути

Име(на) атрибута	OID
commonName, cn	2.5.4.3
surname, sn	2.5.4.4
givenName, gn	2.5.4.42
displayName	2.16.840.1.113730.3.1.241
rfc822Mailbox, mail	0.9.2342.19200300.100.1.3

Напомене:

• Атрибут **commonName** треба да буде конструисан као комбинација имена и презимена особе.

• Ако постоји, атрибут **displayName** се по правилу користи у списковима имена насталим претраживањем; ако не постоји, уместо њега се користи **commonName**.

• Да би се олакшало претраживање, **препоручује** се да атрибути **commonName**, **givenName** и **surname** буду доступни у варијантама: а) изворног језика имена, б) српске латиничне транскрипције са дијакритичким знаковима, в) српске латиничне транскрипције без дијакритичких знакова и г) српске ћириличне транскрипције, с тим да се дупликати не записују посебно.

• Атрибут **mail** треба да садржи примарну електронску адресу особе. Ако овај атрибут има више вредности, клијент је слободан да изабере било коју, па се зато **препоручује** да се атрибут ограничи на јединствену вредност. **Препоручује** се да електронска адреса особе садржи пуно име и презиме запосленог, а не иницијале или псеудониме.

Обавезна функционалност приликом претраживања

Институције које имају студенте морају технички омогућити филтрирање претраге тако да се могу добити скупови записа који се односе на а) све запослене на институцији, б) све активне студенте свих нивоа студија на институцији, и в) комбинацију записа из случајева а) и б). Уколико се филтрирање обавља помоћу специфичних вредности локално дефинисаног атрибута, текстуални запис LDAP филтера за сваки од наведених случајева мора садржати OID представу овог атрибута, а не текстуални еквивалент.