Современные Технологии Федеративного Доступа к Ресурсам Научных и Университетских Сетей

Yuri Demchenko, University of Amsterdam
<demch@science.uva.nl>
Klaas Wierenga, SURFnet
<Klaas.Wierenga@surfnet.nl>

Аннотация
Даный доклад предлагает обзор современных технологий и проектов в области федеративного доступа к сетевым и информационным ресурсам научных и образовательных сетей, которые позволяют использовать единый доступ пользователей к множественным распределенным ресурсам входяшим в федерацию безопасности на основе PKI. Рассматриваются такие технологии и проекты как Shibboleth, AAI/EduGAIN, Eduroam.

1. Введение

Расширение сотрудничества между университетами и научными центрами в Европе и в мире является результатом увеличения наукоемкости современных фундаментальных и прикладных исследований. Это приводит к необходимости обьединения ресурсов сотрудничающих организаций и создания единой федеративной системы доступа для пользователей этих ресурсов. Соответственно это стимулирует развитие новых сетевых технологий и приложений для поддержки такого сотрудничества, которые включают федеративную инфраструктуру управления идентификацией пользователей (Identity Federation), виртуализацию ресурсов и пользовательских групп на основе Грид-технологий, а также поддержку мобильности пользователей.

2. Федеративный доступ к сетевым ресурсам

Под федеративным доступом (Identity Federation, Resource Federation, Federated access) понимается комплекс технологий и соответствующая инфраструктура, которые позволяют использовать единое имя пользователя и/или его мандат/сертификат идентификации для доступа в сетях, которые установили между собой доверительные отношения и входят в ассоциацию безопасности, обычно называемую «федерацией» [1]. Доверительные отношения (или доверие) обычно устанавлиется на основе Системы Открытых Ключей (СОК, или PKI – Public Key Infrastructure).

Технология и инфраструктура федеративного доступа к сетевым ресурсам приобретает все большее распространение как в среде научных и образовательных сетей, где она является насущной необходимостью для поддержки научного сотрудничества, так и для коммерческих сетей и приложений, где она обещает существенную экономию затрат на администрирование пользовательского доступа в распределенных приложениях.

Проблема федеративного доступа к распределенным ресурсам фактичеки распадается на две взаимовязанные проблемы: поддержка федераций организаций и пользователей и обеспечение взаимного доступа пользователей к ресурсам организаций, котрые входят в так-называемые федерации.

Первая проблема создания и поддержки федераций организаций и пользователей фактически решается посредством установления доверительных отношений между системами идентификации пользователей (IdP - Identity Provider), имеющимися в наличии в «домашних» организациях и сетях пользователей.

Такие федерации IdP позволяют использовать удаленную сетевую аутентификацию пользователей в «домашней» организации в случае, если пользователь запрашивает доступ к сети или другим ресурсам из организации, входящей в федерацию. Дополнительно, федерации IdP позволяют также

обмениваться характеристиками пользователей (обычно называемыми «атрибутами»), которые используются для определения уровня доступа или категории сервисов и ресурсов, которые доступны пользователю.

3. Популярные платформы и инфраструктуры для федеративного доступа

Две основные платформы, используемые в научных и университетских сетях для создания инфраструктуры федерации IdP, являются Shibboleth [2], изначально разработанная Intenet2, и A-Select [3], разработанная SURFnet. Обе платформы являются свободно распространяемыми и имеют обширную международную пользовательскую базу. Целесообразно также отметить, что популярным решением для единого доступа в коммерческом мире является система единого доступа SSO (Single Sign-On), разработанная в рамках Liberty Alliance Project (LAP) [4].

Важным отличием между между двумья типами решений является то, что Shibboleth и A-Select в первую очередь расчитаны на доступ к веб-ресурсам посредством броузера, в то время как LAP в основном предлагает решение для приложений на основе Веб-сервисов (Web Services). Важно также отметить, что основой и условием для федерации IdP является наличие развернутой инфраструктуры Системы Открытых Ключей (СОК или PKI – Public Key Infrastructure). В то же время нужно также отметить, что стандартом для обмена сертификатами или мандатами между компонентами системы единого доступа является SAML (Security Assertions MarkUp Language) [5].

Распределенный доступ к федеративным ресурсам использует инфраструктуру поддержки федераций пользователей, но требует соответствующую организацию системы аутентификации (AuthN – Authentification) авторизации (AuthZ - Authorisation), контролирующих доступ к собственно ресурсам как сетевым, так и к специальным приложениям. Создание федеративной инфраструктуры аутентификации и авторизации, известной как AAI, является одной из важнейших инициатив Европейских научных сетей. Находящийся в настоящее время на этапе внедрения проект eduGAIN (GEANT Authorisation Infrastructure for the research and education community) ставит своей задачей создание федеративной AAI в Транс-Европейской научной сети GEANT [6].

Многие Европейские научные сети предоставляют услуги поддержки национальных федераций или создания целевых федераций посредством предоставления услуг третьей доверительной стороны для обмена пользовательскими данными, необходимыми для контроля доступа пользователей к федеративным ресурсам. Примерами могут быть SURFnet Federation (SURFnet, The Netherlands) [7], SWITCHaai (SWITCH, Switzerland) [6], а также InCommon/MACE Federation в США на основе Shibboleth [9].

Особой популярностью пользуется инфраструктура распределенного доступа мобильных пользователей Eduroam (Education Roaming) [10]. Инициатором Eduroam стали SURFnet и целевая группа по вопросам мобильности Ассоциации Европейских научных сетей TERENA [11]. В настоящее время федеративная инфраструктура Eduroam включает 22 Европейские страны, Австралию, Тайвань, а также отдельные университеты в США. Пользователи из сетей и организаций, входящих в федерацию Eduroam, могут использовать свой постоянный логин (имя пользователя и пароль в своей «домашней» организации) для доступа к Интернет в любой сети федерации Eduroam. Это создает реальную платформу для мобильности пользователей, и в частности, для обмена учебными программами между университетами.

Eduroam использует протокол RADIUS (Remote Authentication Dial In User Service) для удаленной аутентификации пользователей, который в настоящее время используется многими университетами в Росии, однако для включения в федерацию Eduroam необходимы также широкое внедрение СОК и установление доверительных отношений между национальными Сертификационными центрами СОК, что в свое время потребует гармонизации политики сертификации СОК российских центров сертификации и сетей или стран членов федерации Eduroam.

4. Федеративный доступ к распределенным ресурсам в Грид

Федеративный доступ к виртуализованным компьютерным ресурсам по сути является основой инфраструкуры безопасности и контроля доступа в Грид. Федерации пользователей и ресурсов в Грид, как правило, ориентированы на отдельные научно-иследовательские проекты и являются более динамичными, чем университетские федерации, и имеют форму Виртуальных Организаций (ВО). Стандартом де-факто для поддержки ВО является служба VOMS (Virtual Organisations Membership Service) [12], которая предоставляет пользовательские атрибуты для систем контроля доступа (или авторизации) к Грид-ресурсам.

В настоящее время имется несколько инициатив, направленных на интеграцию и взаимодействие инфраструктуры ВО и федеративных IdP [13]. Пограммное обеспечение VOMS Attributes from Shibboleth (VASH) [14], разрабатываемое в рамках проекта EGEE (Enabling Grids for E-sciencE) [15], позволит взаимно использовать атрибуты ВО и Shibboleth для контроля доступа в Грид.

5. Заключение

Внедрение технологий федеративного доступа является необходимым компонентом интеграции российских научных сетей в европейские и международные научные сети.

Европейские и зарубежные университеты и научные сети прошли большой путь от создания высокоскоростной транспортной сетевой инфруктуры до создания инфраструктуры поддержки распределенных приложений (часто называемой middleware) и распределенной системы доступа пользователей к этим ресурсам. Изучение этого опыта и внедрение соответствующих технологий российскими университетами позволит создать базу как для более тесного сотрудничества между российскими организациями, так и для расширения междурародного сотрудничества.

Литература

[1] Report Federated Identity Management in Higher Education – http://aaa.surfnet.nl/info/en/artikel_content.jsp?objectnumber=182026

[2] Shibboleth- http://shibboleth.internet2.edu/

[3] A-Select Authentication System. - http://aaa.surfnet.nl/info/a-select/home.jsp

[4] eduGAIN: Federation Interoperation by Design - http://www.terena.org/events/tnc2006/programme/presentations/show.php?pres_id=202

[5] SURFnet Federation - http://federatie.surfnet.nl/cms/

[6] SWITCHaai - http://www.switch.ch/aai/

[7] MACE InCommon Federation. - http://www.incommonfederation.org/

[8] Eduroam - http://www.eduroam.org/

[9] TF-EMC2 - http://www.terena.org/activities/tf-emc2/

[10] Liberty Alliance Project. - http://www.projectliberty.org/

[11] Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005. [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[12] Virtual Organization Membership Service (VOMS) - http://littleblue.cnaf.infn.it/twiki/bin/view/VOMS/WebHome?

[13] Case Studies for Identity Management for Virtual Organizations, Southwest Regional Conference 2007, February 2007. - http://educause.edu/ir/library/pdf/SWR07058.pdf

[14] VOMS Attributes from Shibboleth (VASH). JRA1 All-Hands meeting, 7-9 March 2007. [Online]. Available: http://indico.cern.ch/getFile.py/access?contribId=34&sessionId=2& resId=1&materialId=slides&confId=11908

[15] The Enabling Grids for E-sciencE project. - http://www.eu-egee.org/