

# СЕРВИСЫ ФЕДЕРАТИВНОЙ АВТОРИЗАЦИИ – ПУТИ РАЗВИТИЯ

25.06.2013

XI МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ  
КОНФЕРЕНЦИЯ И ВЫСТАВКА «КОРПОРАТИВНЫЕ  
БИБЛИОТЕЧНЫЕ СИСТЕМЫ: ТЕХНОЛОГИИ И  
ИННОВАЦИИ»

---

# Книга Судей Израилевых, Глава 12, стихи 5-6

<sup>5</sup> И перехватили Галаадитяне переправу чрез Иордан от Ефремлян, и когда кто из уцелевших Ефремлян говорил: "позвольте мне переправиться", то жители Галаадские говорили ему: не Ефремлянин ли ты? Он говорил: нет.

Суд 3:28  
Суд 7:24  
Ис Нав 22:11

<sup>6</sup> Они говорили ему "скажи: шибболет", а он говорил: "сибболет", и не мог иначе выговорить. Тогда они, взяв его, закололи у переправы чрез Иордан. И пало в то время из Ефремлян сорок две тысячи.

---

Вход в библиотеку

IP-адрес компьютера:  
212.116.105.240

Название организации:  
не определена

Имя пользователя:

Пароль:

**Вход**

Запомнить меня

✉ Почта

@mail.ru ▾

**Войти**

Забыли пароль?  запомнить

Регистрация в почте  
с безлимитным ящиком

Ваш IP-адрес: 212.116.105.240

Библиотека не определена

Логин

Пароль  **войти**

[Забыли пароль?](#) [Регистрация](#)

### ВХОД В СИСТЕМУ

ЛОГИН

ПАРОЛЬ  **ВОЙТИ**

№ Абонента

Имя пользователя

Пароль

[Забыли пароль?](#)

**OK** **отмена**

**Айбукс**

**Авторизация**

Логин

Пароль

**Вход**

[Забыли пароль?](#)

# ПРОБЛЕМЫ

- Утомительная регистрация в большом количестве ресурсов, хранение учетных данных пользователя для каждого ресурса.
  - Наличие ненадежных и устаревших данных о пользователях в самих ресурсах.
  - Обезличенный процесс доступа при авторизации по IP адресам организации, проблемы смены IP.
  - Риски нарушения законодательства о защите персональных данных.
-

# ИСТОРИЯ СИСТЕМ ИДЕНТИФИКАЦИИ

- Изолированные аккаунты
  - Централизованные базы данных пользователей
    - LDAP, SQL
  - Технологии единого входа
    - Kerberos, PKI и др.
  - Федеративная авторизация
    - SAML, OpenID, Shibboleth
-

# ФЕДЕРАТИВНАЯ ИДЕНТИФИКАЦИЯ

- Это обобщение алгоритмов единого входа
  - Нет жесткой привязки источников данных о пользователях к приложениям или службам
  - Нет предположений о доверии к источникам данным
-

שִׁבּוֹלֵת

(ШИБОЛЕТ)

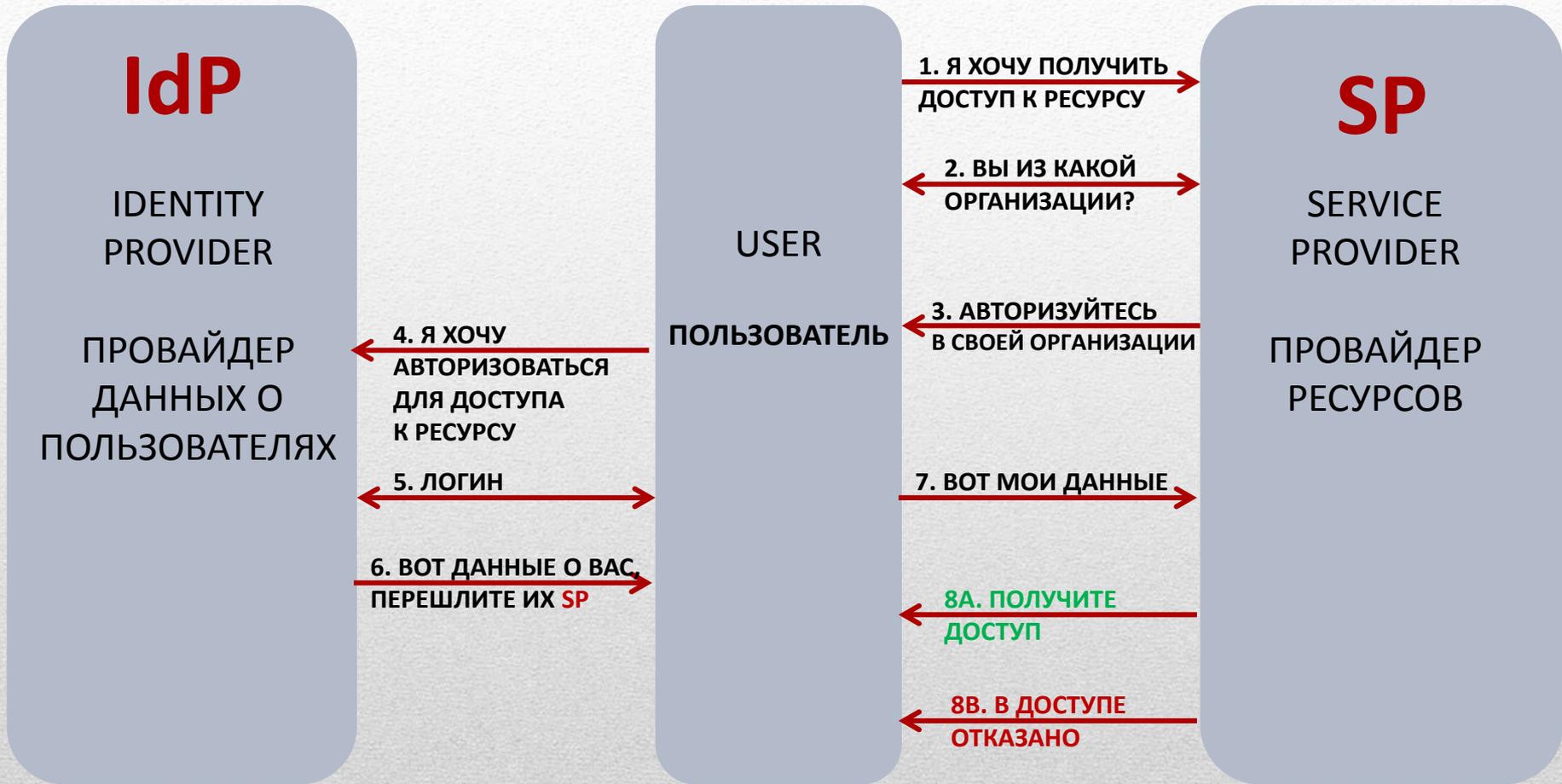
---

# Security Assertion Markup Language (SAML)

*Дословно: «Язык разметки утверждений о безопасности».*

XML-протокол обмена токенами безопасности между SAML-источником IdP (провайдером данных о пользователях) и SAML-клиентом SP(провайдером ресурсов)

---

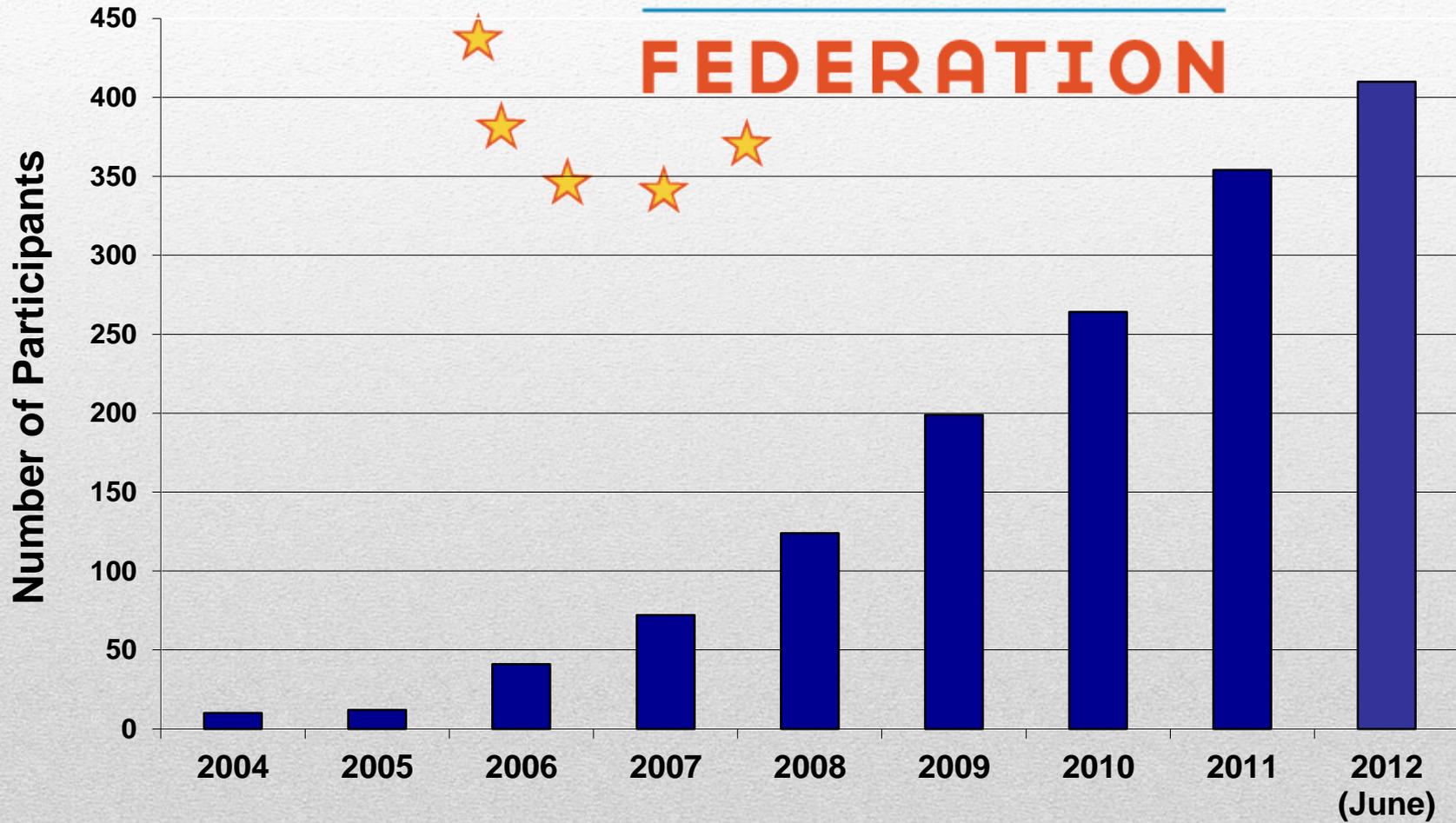


# ФЕДЕРАЦИЯ ДОСТУПА

- Регистрация пользователя происходит только один раз, а именно в «Домашней Организации»
  - Процесс аутентификации всегда выполняется Домашней Организацией пользователя, все ресурсы Федерации доступны пользователям с единственным набором учетных данных.
  - У операторов ресурсов нет потребности в регистрации новых пользователей, необходимую информацию они получают от Домашней Организации пользователя.
  - Правила доступа, формируемые Ресурсом, базируются на получаемой информации о пользователе.
-

# InCommon®

## FEDERATION



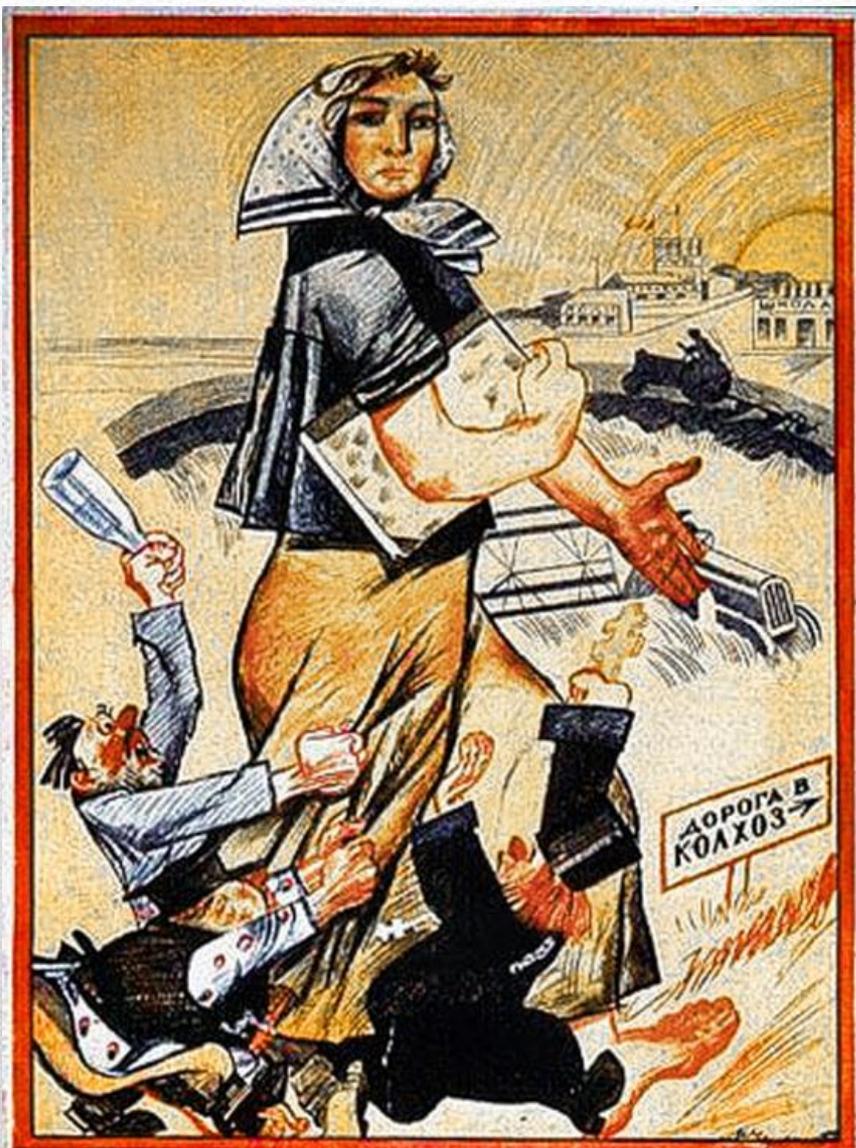
# ФЕДЕРАЦИЯ ДОСТУПА

- Регистрация пользователя происходит только один раз, а именно в «Домашней Организации»
  - Процесс аутентификации всегда выполняется Домашней Организацией пользователя, все ресурсы Федерации доступны пользователям с единственным набором учетных данных.
  - У операторов ресурсов нет потребности в регистрации новых пользователей, необходимую информацию они получают от Домашней Организации пользователя.
  - Правила доступа, формируемые Ресурсом, базируются на получаемой информации о пользователе.
-

# ФЕДЕРАЦИЯ ДОСТУПА

## *φEDUrus*

- использует данную технологию, гарантируя каждому участнику федерации сохранение функций, относящихся к нему:
    - Домашние Организации регистрируют и подтверждают подлинность своих членов
    - Администраторы Ресурсов определяют свои правила доступа
  - φEDUrus , с другой стороны, управляет центральными компонентами AAI инфраструктуры и осуществляет поддержку Домашних Организаций и Ресурсов.
-



BCE

B

*φEDUrus!*

# БЛАГОДАРНОСТИ

Максиму Бутову

Ведущему техническому специалисту  
Научной Библиотеки СЗИУ РАНХиГС

Коллегам из организаций

TERENA (<http://www.terena.org/>)

и

JISC (<http://www.jisc.ac.uk/>)

---

**Соколов Андрей Владимирович**

Заместитель директора

Научная библиотека им. М. Горького

Санкт-Петербургский государственный университет

andrew@lib.pu.ru

+7 (812) 328-95-46

**Порхачёв Василий Александрович**

pva@ibooks.ru

+7 (812) 7037372 #6226

**СПАСИБО!**

---