R·Style

# Обеспечение аутентификации и авторизации в Интернет: роль УЦ и электронного правительства

Михаил Ванин
Начальник отдела разработки
систем идентификации и аутентификации

конференция РусКрипто

# Сближение инфраструктур

# Сближение инфраструктур


Основные системы:

- Портал государственных услуг (ЕПГУ).
- Система межведомственного электронного взаимодействия (СМЭВ).
- Единая система идентификации и аутентификации (ЕСИА).
- Информационная система головного удостоверяющего центра (ИС ГУЦ).

R·Style

# Сближение инфраструктур


Факторы сближения:

- Развитие электронных услуг и межведомственного взаимодействия.
- Изменения в нормативной базе.
- Введение «электронных» удостоверений личности граждан РФ.

# Результат слияния инфраструктур


- Обеспечивает достоверную идентификацию субъектов взаимодействия (индивидумы, организации, информационные системы, электронные устройства).
- Обеспечивает получение данных о субъектах и авторизацию при взаимодействии.

# Роль инфраструктуры УЦ в будущей экосистеме

## Уменьшение роли

### Обеспечение идентификации

- ФМС будет выдавать гражданам паспорт с КЭП «на борту».
- УЦ как сеть электронной регистрации пользователей будет менее востребован (не выдержит конкуренции с ФМС).
- Произойдет унификация форматов сертификатов из различных пространств доверия.

## Увеличение роли

### Обеспечение авторизации

- УЦ продолжат «удостоверять» полномочия владельцев средств ЭП.

  Но делать это будут по-новому.
- Кол-во электронных взаимодействий, а с ними и роль достоверной электронной авторизации значительно возрастут.

## Подход 1. УЦ ведет данные авторизации

### Варианты реализации

- Полномочие определяется пространством доверия.

  Пользователь имеет полномочие, если сертификат выдан определенным УЦ.
- В сертификаты добавляют специальные OID, кодирующие полномочия (характерный пример – OID для Росреестра).

### Недостатки

- Низкая оперативность обновления данных о полномочиях.
- Сложность отзыва полномочия.

## Подход 2. Поставщик услуги ведет данные авторизации

### Варианты реализации

- Перед использованием поставщика услуг пользователь должен пройти в нем регистрацию.
- Поставщик услуг для проверки полномочий вызывает сторонние источники достоверных данных о пользователе (пример - проверка в ЕГРЮЛ).

### Недостатки

- В каждом поставщике услуг пользователю (и его организации) приходится по своему вести полномочия.
- Поставщик услуг вынужден решать непрофильные задачи.
- Сложность отзыва полномочия.

## Подход 3. Полномочия ведутся в ЕСИА

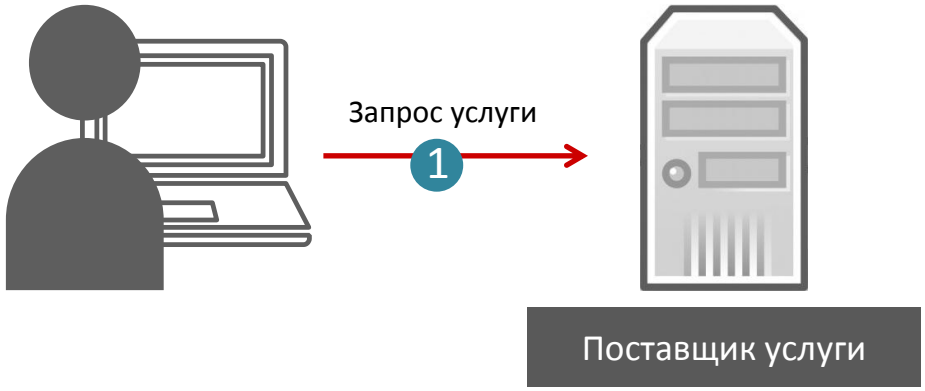
### Варианты реализации

- Ответственный сотрудник регистрирует ЮЛ/ОГВ в ЕСИА, присоединяет к ЮЛ/ОГВ сотрудников, делегирует им полномочия относительно зарегистрированных в ЕСИА систем.

### Недостатки

- ЕСИА обслуживает только поставщики услуг гос. организаций.
- Низкая оперативность обновления данных о полномочиях.
- ЕСИА не позволяет делегировать проверку полномочий 3 стороне (кому-то кроме поставщика услуг или организации, где работает сотрудник).

# Перспективное решение – экосистема с поставщиками атрибутов



# Перспективное решение – экосистема с поставщиками атрибутов

Запрос услуги

1

Поставщик услуги

2

Поиск ИС, которая предоставит необходимые атрибуты

Сервис авторизации

Поставщик идентификации

Регистр атрибутов

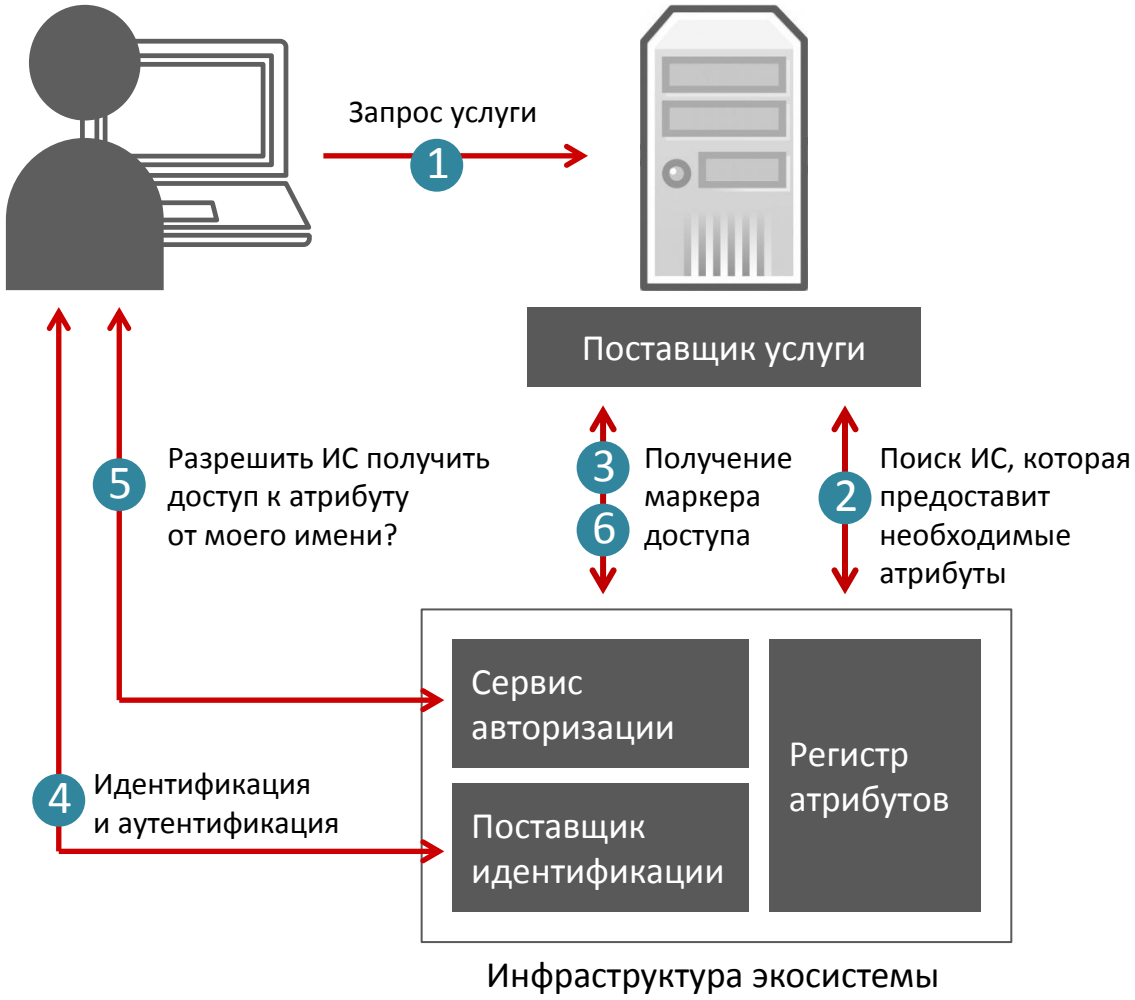
Инфраструктура экосистемы

Поставщики атрибутов государственных организаций

Поставщики атрибутов некоммерческих организаций

Поставщики атрибутов коммерческих организаций

# Перспективное решение – экосистема с поставщиками атрибутов




Поставщики атрибутов государственных организаций

Поставщики атрибутов некоммерческих организаций

Поставщики атрибутов коммерческих организаций

# Перспективное решение – экосистема с поставщиками атрибутов

# Текущее состояние развития инфраструктуры экосистемы

| Элемент инфраструктуры | Текущее состояние и планы |
|---|---|
| Поставщик идентификации | ЕСИА в основе.<br>Кол-во пользователей:<br>• Более 8 млн граждан;<br>• Более 50 тыс. ЮЛ.<br>Технологии для взаимодействия:<br>• SAML 2.0;<br>• Open ID Connect. |
| Сервис авторизации | ЕСИА в основе.<br>Сейчас используется для контроля доступа к программным интерфейсам REST-API самой ЕСИА.<br>Будет развиваться для использования сторонними системами.<br>Технологии для взаимодействия:<br>• OAuth 2.0. |
| Регистр атрибутов | Пока не создан.<br>Развитие на базе одной из систем: ЕСИА, СМЭВ, ИС ГУЦ. |

R·Style

# Возможная роль УЦ в экосистеме

## УЦ как поставщик атрибутов

- В офисах УЦ проверяется наличие у пользователя полномочий. Пользователям присваиваются достоверные атрибуты. Информация об атрибутах пользователя помещается в базу УЦ.
- УЦ публикует в экосистеме свой поставщик атрибутов.

## УЦ как посредник

- УЦ реализует интеграцию с ИС своих партнеров.
- УЦ публикует в экосистеме поставщик атрибутов как интерфейс к данным из ИС партнеров.

# Благодарим за внимание и приглашаем к сотрудничеству!

Михаил Ванин
mikhail.vanin@r-style.com
+7 (964) 626 20-69

123022, г. Москва, ул. Рочдельская, д.15, к.16а
+7 (495) 640 60-10
www.r-style.com