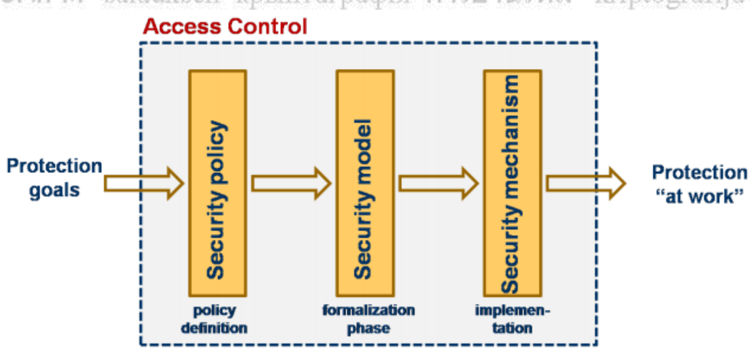
Инфраструктура управления полномочиями

Способы построения



Павел Смирнов

ООО «КРИПТО-ПРО»

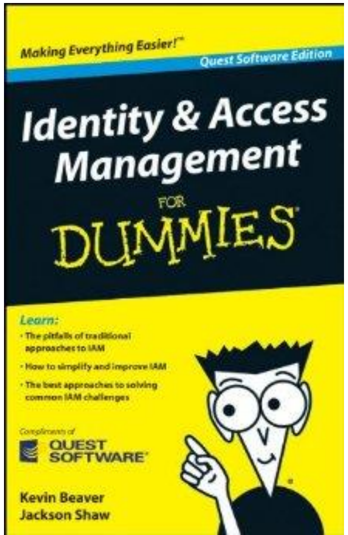
О чем пойдёт речь

- Что такое инфраструктура управления полномочиями
- Задача управления полномочиями, подходы к решению
- Современные стандарты
  - Атрибутный сертификат X.509
  - SAML
  - OAuth 2.0
- Перспективы использования в России

Инфраструктура управления полномочиями

Инфраструктура управления полномочиями (**Privilege Management Infrastructure**) – система управления процедурами авторизации пользователей, основанная на стандартах и рекомендациях, к которым относятся:

- RFC 5755, An Internet Attribute Certificate Profile for Authorization;
- ITU-T Recommendation X.1254 | International Standard ISO/IEC DIS 29115 Information technology — Security techniques — Entity authentication assurance framework;
- ITU-T Recommendation X.509. Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks.



Авторизация

Современные операционные системы имеют интегрированные механизмы авторизации пользователей

win

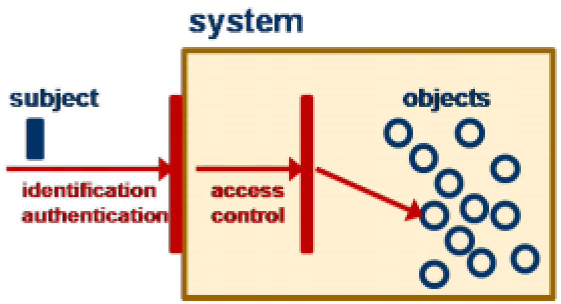
– Active Directory LDAP

unix

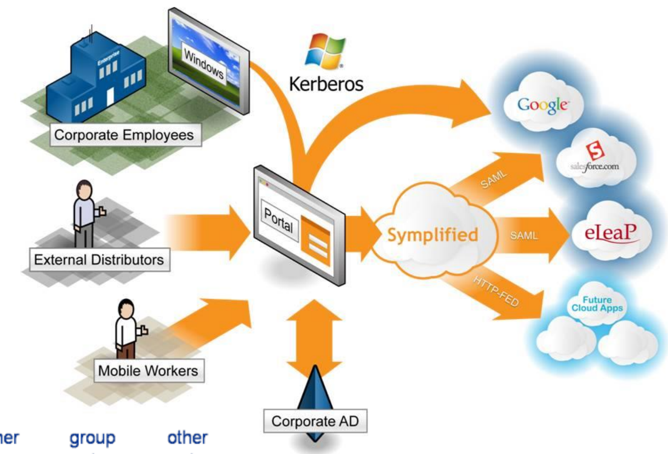
– /etc/passwd and /etc/group (default)
– LDAP-compatible directories (нр. iPlanet)
– NIS, NIS+

Встроенные механизмы авторизации не применимы:

- на уровне приложений
- в распределенных разнородных информационных системах



Разнородные системы



субъекты

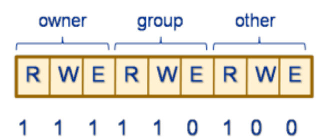
- не совпадают с учётными записями ОС

объекты

- не соответствуют объектам ОС (нр. файлы)

права

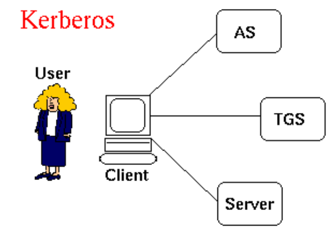
- отличаются от принятых в ОС прав (нр. Read, Write, eXecute)



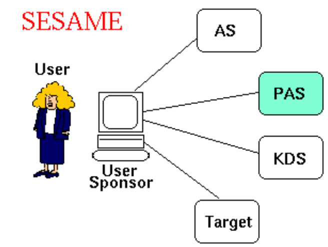
инфраструктура авторизации – сложная комплексная система

разработчики приложений либо сводят процесс авторизации к методам ОС, либо придумывают все новые и новые решения

Попытки



DCE: Registration Service (RS), Key Distribution Service (KDS), Privilege Service (PS)



SESAME: Kerberos, PKI, Privilege Attribute Certificates

CORBA (Common Object Request Broker Architecture):
IIOP (Internet InterORB Protocol), DCE | SESAME

Object Control Attributes

General form:
```
if [condition]
then
    [subject] [may | may not]
    do [action] to [object]
```

Capability form:
```
if [condition]
then
    this-subject [may | may not]
    do [action] to [object]
```

ACL form:
```
if [condition]
then
    [subject] [may | may not]
    do [action] to this-object
```

Современные стандарты

X.509 Attribute Certificate

- RFC 5755, An Internet Attribute Certificate Profile for Authorization;
- ITU-T Recommendation X.509. Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks;
- ETSI TS 102 158 Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates.

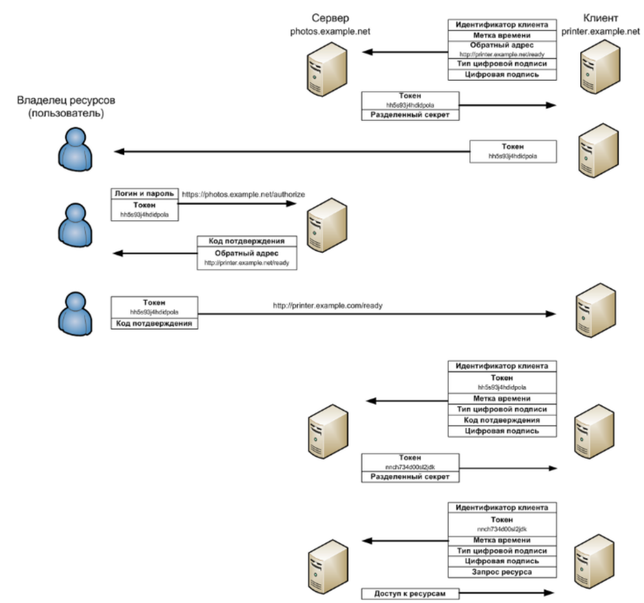
SAML (Security Assertion Markup Language): XML authorization framework

- XACML, XrML

Identification	WS-Security Framework
Authentication	Extensible Access Control Markup Language (XACML)
Authorization	Extensible Rights Markup Language (XrML)
	XML Key Management (XKMS)
	Security Assertion Markup Language (SAML)
	.NET Passport

OAuth 2.0

- RFC 6749 The OAuth 2.0 Authorization Framework
- RFC 6750 The OAuth 2.0 Authorization Framework: Bearer Token Usage



Поля X.509 Attribute Certificate (AC)

```
AttributeCertificateInfo ::= SEQUENCE {
    version                 AttCertVersion,
    holder                  Holder,
    issuer                  AttCertIssuer,
    signature               AlgorithmIdentifier,
    serialNumber            CertificateSerialNumber,
    attrCertValidityPeriod  AttCertValidityPeriod,
    attributes              SEQUENCE OF Attribute,
    issuerUniqueID          UniqueIdentifier OPTIONAL,
    extensions              Extensions OPTIONAL
  }
```

Примеры атрибутов в АС

RFC 5755 An Internet Attribute Certificate Profile for Authorization

Вместо открытого ключа в АС атрибуты:

- Service Authentication Information
- Access Identity
- Charging Identity
- Group
  - name
  - OID
  - syntax
  - values
- Role
  - roleAuthority
  - roleName
    - OID
    - syntax
    - values
- Clearance
  - unclassified (1),
  - restricted (2),
  - confidential (3),
  - secret (4),
  - topSecret (5)

Концепция АС

- Связь с сертификатом X.509
- Непрямая идентификация
- Указание издателя
- Шифрование атрибута
- Аннулирование АС (ACRL)
- Верификация издателя
- Короткое время жизни АС
- АС на проверку может браться:
  - От владельца АС в составе протокола
  - От издателя АС

X.509 AC: итого

Несмотря на наличие стандартов (с 1997г.):

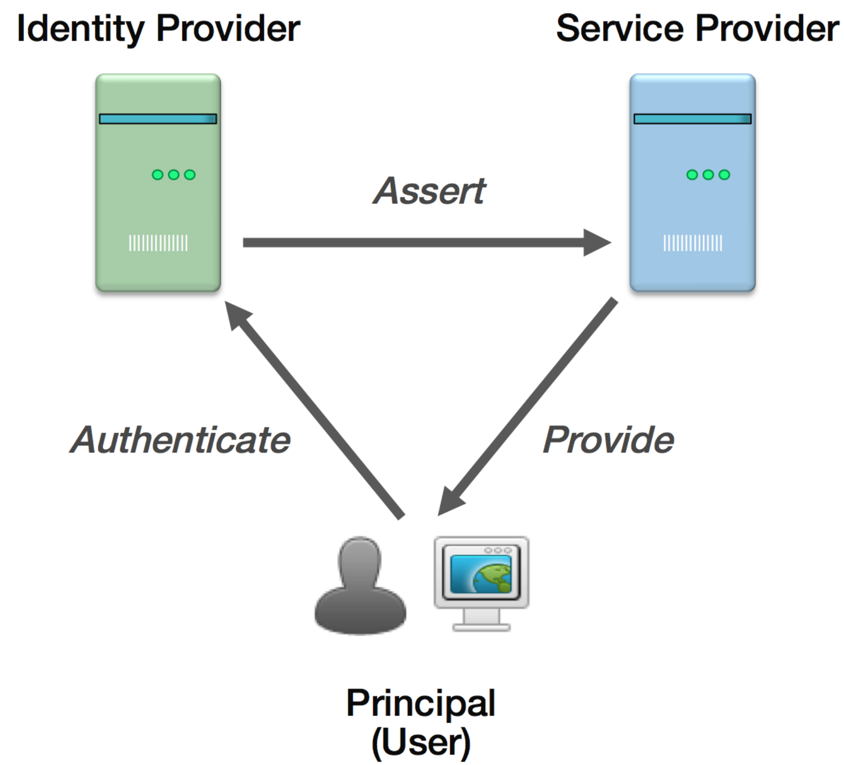
- RFC 5755 An Internet Attribute Certificate Profile for Authorization
- X.509 Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks

отсутствует реализация и поддержка в протоколах, приложениях, средствах разработки (веб-сервисы, Java, .NET, C/C++)

SAML

Стандарты OASIS (с 2002 г.)

- Security Assertion Markup Language (SAML)
- Web Services Security Policy Language (WS-SecurityPolicy)
- Web Services Metadata Exchange (WS-MetadataExchange)
- Web Services Trust Language (WS-Trust)
- Web Services Federation Language (WS-Federation)



Поддержка

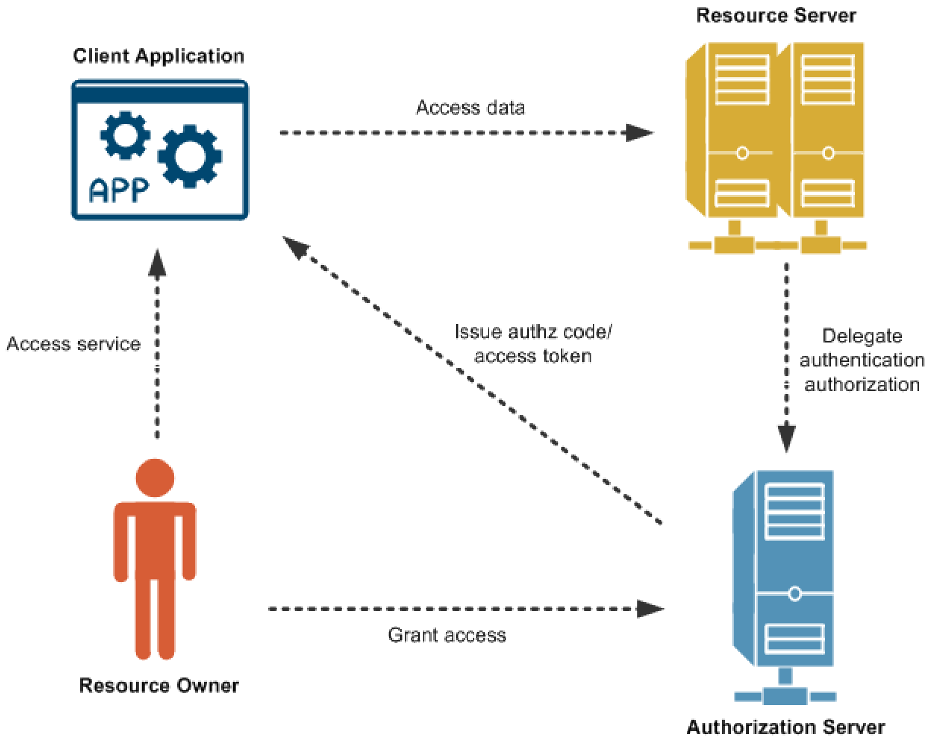
- Вендоры: Microsoft, Citrix, HP, Intel, IBM, VMware, Oracle, RSA, Amazon, Google, Salesforce, …
- Библиотеки для: C/C++, Python, Java, Perl, Ruby, PHP, .NET, ASP.NET, Node.js, …

Формат токена: XML

OAuth 2.0

Спецификации (с 2010 г.):

- RFC 6749 The OAuth 2.0 Authorization Framework
- RFC 6750 The OAuth 2.0 Authorization Framework: Bearer Token Usage
- RFC 7519 JSON Web Token
- OpenID Connect Core 1.0



Поддержка

- Вендоры/сайты: Microsoft, Intel, Amazon, Dropbox, Evernote, Facebook, Google, Instagram, Twitter, Salesforce, …
- Библиотеки для: C/C++, Python, Java, Ruby, PHP, .NET, ASP.NET, Node.js, JavaScript, …

Формат токена: JSON

Настоящее и будущее

РОСРЕЕСТР
Федеральная служба государственной регистрации, кадастра и картографии

Аккредитованные УЦ (368 или 387?)

ПЕРЕЧЕНЬ УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ, ИСПОЛНИВШИХ ТРЕБОВАНИЯ РАСПОРЯЖЕНИЯ РОСРЕЕСТРА ОТ 27.03.2014 № Р/32

<u>(квалифицированный сертификат с дополнениями – 45(!) разных объектных идентификаторов)</u>

- УЦ «ТехноКад»
- УЦ ООО «Электронные Бизнес Системы»
- НП «МосГорУслуга»
- . . .
- Государственное казенное учреждение "Ресурсы Ямала"

Операторы (XXX)

ПЕРЕЧЕНЬ ОПЕРАТОРОВ ИНФОРМАЦИОННЫХ СИСТЕМ (ЮРИДИЧЕСКИХ ЛИЦ), ВЫДАЮЩИХ СЕРТИФИКАТЫ АТРИБУТОВ

<u>(сертификат атрибутов)</u>

кто все эти люди

какой УЦ выдал сертификат для создания АС

как проверить подпись АС

ЕСИА

Из Приказа Минкомсвязи России от 13.04.2012 №107 (о ЕСИА):

1.5. Единая система идентификации и аутентификации обеспечивает осуществление следующих функций:

б) **аутентификация** сведений об участниках информационного взаимодействия … в том числе с использованием квалифицированных сертификатов ключей проверки электронных подписей …;

в) **авторизация** участников информационного взаимодействия … в части ведения и **предоставления информации о полномочиях** участников информационного взаимодействия в отношении информационных систем …;

3.7. В регистре информационных систем оператором единой системы идентификации и аутентификации указываются сведения об информационных системах …

Полномочия в единой системе идентификации и аутентификации для функционирования указанных информационных систем устанавливаются электронными сервисами операторов информационных систем - поставщиков информации - для межведомственного электронного взаимодействия, для реализации иных целей - в соответствии с действующим законодательством.

Поддерживает SAML и OAuth

Заключение

- Определение прав пользователей в информационных системах – сложная комплексная задача, которая должна решаться совместно информатизаторами и безопасниками.
- Формат «токена с полномочиями» – второстепенный вопрос.

- Внедрение X.509 AC
  - выгодно:
    - разработчикам – новые продукты, тираж
    - интеграторам – новые внедрения, модернизация ИС
  - невыгодно:
    - бюджету оператора ИС
    - бюджету пользователя – ему за все придется заплатить
- Внедрение SAML, OAuth
  - уже есть, доработка ЕСИА в части нормативных требований и расширения атрибутов