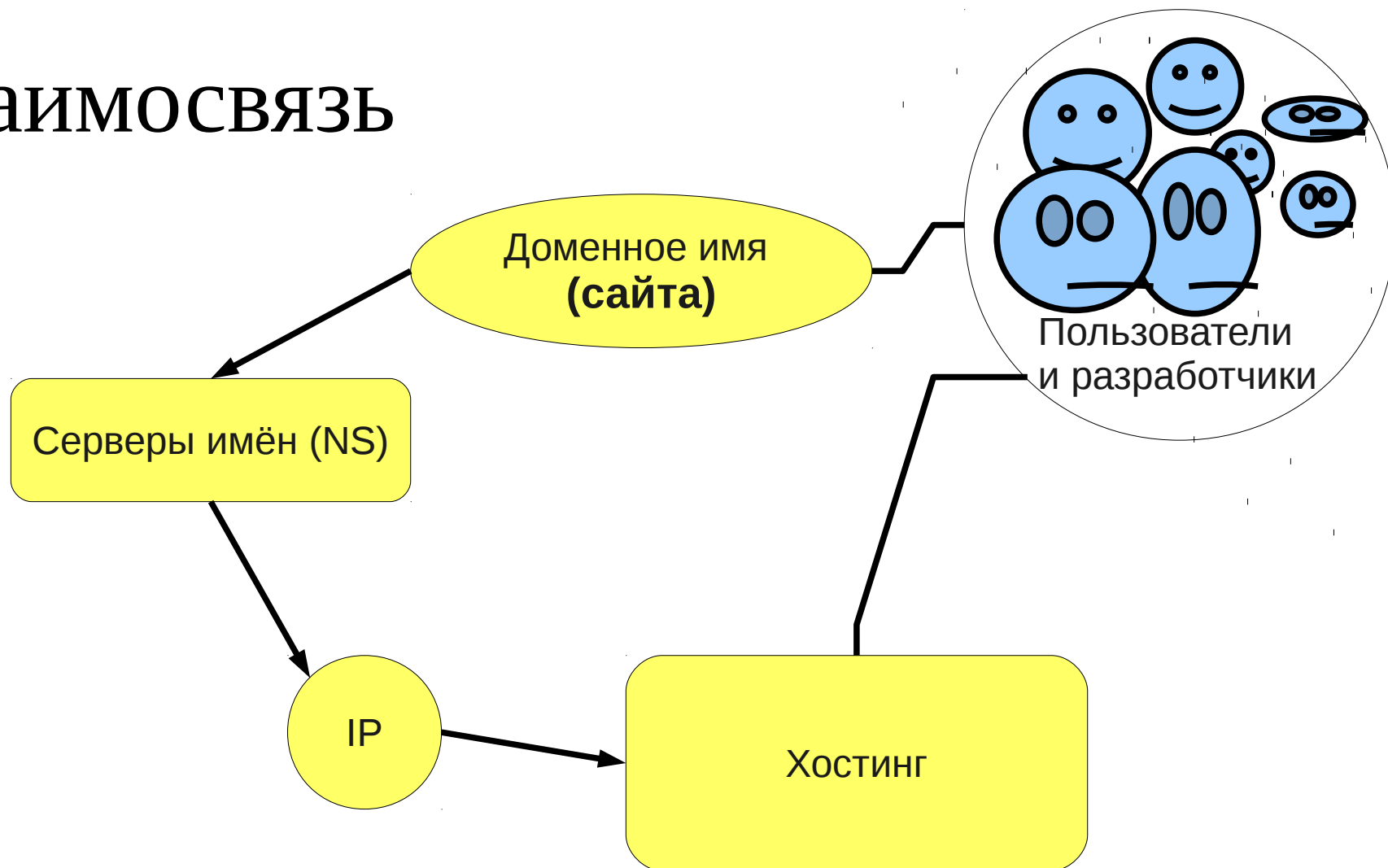




Сопровождение домена и безопасность

Александр Венедюхин,
«Доменные имена»

Взаимосвязь



Базовые навыки

Пароли - не хранить в открытом виде;

Обновления ПО, отсутствие «троянов»;

Открытые сети использовать с осторожностью;

Нет FTP - только SSH (SFTP);

«Админка» CMS только через HTTPS;

и т. д., и т. п.

Атаки на домены – почему?

Основа пользовательской навигации

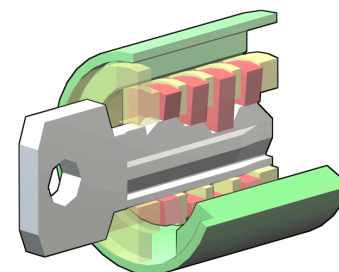
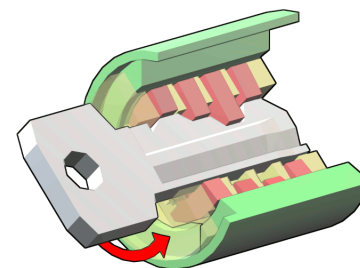
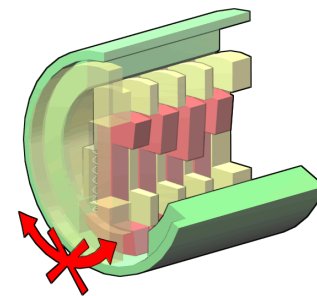
Не требуется ломать сайт - *сломайте домен.*

Домен «сломан»:

**пользователи отправляются куда угодно
(*...и вводят, и вводят свои данные*).**

Атаки на домены

- 1) взлом NS-ов;
- 2) перехват управления;
- 3) взлом регистратора.



Атаки на домены

(непрямые)

- 1) «угон» домена;
- 2) «обратный захват».

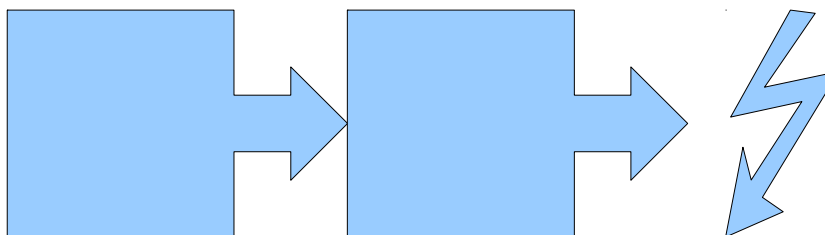
Регистрация опечаток — «параллельная» атака.



Атаки на домены

Технические направления «второго порядка»:

- 1) перехват домена контактной почты;**
- 2) взлом/«инфицирование»/«отравление» элементов DNS.**
(у провайдера, на клиенте)



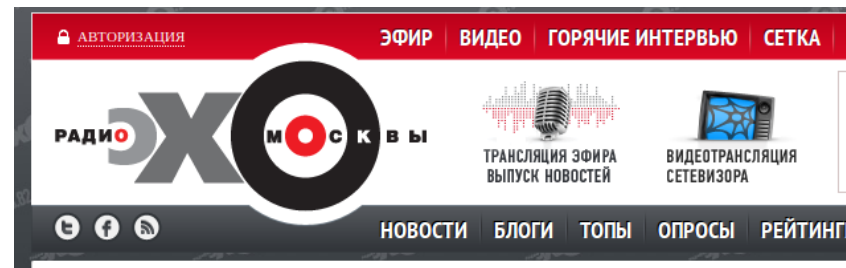
Реальность

Сентябрь 2011 года:

домены, зарегистрированные NetNames - смена NS-ов.

**среди этих доменов: theregister.co.uk, telegraph.co.uk,
vodafone.com, acer.com, nationalgeographic.com**

Реальность



Март 2012 года:

атака на серверы RU-CENTER -> проблемы у «Эха Москвы»
(а сайт работал!)

оперативно нарастили мощности

зомби

Зомби против воли

**Владельцы решили отказаться от сайта. Хостинг — удалили.
Домен — не продлили.**

Вуду:

- 1) подхватить освободившийся домен;**
- 2) достать страницы сайта из хранилищ и кэшей (Archive.org, например);**
- 3) --- зомби работают бесплатно (ссылки, SEO и т.п.)!**

Опять практика

Примеры

Получение доступа к панели управления:

- 1) подбор пароля, перехват трафика;**
- 2) фишерские ссылки (в сообщениях e-mail, в интернетовских соц. сетях, на форумах и т. п.);**
- 3) «подхват» почтовых адресов с запросом на восстановление пароля (массовые попытки).**

Дополнительные проверки



Центр
регистрации
доменов

» Домены
» Аукцион

» Почта
» Хостинг

» DNS-серверы
» Паркинг

» SSL-сертификаты

Для клиентов: [Вход](#) 
[Стать клиентом](#) [Напомнить](#)

[О компании](#) | [Услуги](#) | [Договор](#) | [Тарифы и оплата](#) | [Партнерские программы](#)

[Блог](#)

Если Вы забыли административный пароль или номер договора

■ По клиентскому договору или анкете (NIC-D)

1. Пароль может быть восстановлен по [официальному письму](#).
2. Пароль может быть выслан по электронной почте на адрес, указанный в поле «e-mail» договора, **если Вы это предварительно не запретили**.

Для получения пароля по электронной почте заполните форму:

Восстановить пароль по:

- ☒ домену или идентификатору хостинга
☐ номеру договора
☐ домену на паркинге

Домен или идентификатор хостинга:

Дата рождения (для физ. лиц и ИП):
или

(ДД.ММ.ГГГГ)

ИНН (для юридических лиц,
резидентов РФ):

[Выслать данные →](#)

■ По партнерским договорам (NIC-REG, NIC-A)

Административный пароль восстанавливается только по [официальному письму](#)

Напоминаем, что, в соответствии с договором, Заказчик обязуется «самостоятельно нести риск возможных неблагоприятных для него последствий, связанных с утерей и(или) разглашением пароля».

Что делать

(кроме очевидного)

Информированность

Включить все доступные уведомления (e-mail, SMS, IM и др.)

Наладить разумный мониторинг (cron, wget и т.п.)



Регламент

**Что,
как,
кто
делает, если «инцидент произошел»**

адреса, пароли, явки



Фото: futureshape, flickr.com

DNSSEC

(Защищает только от подмены адресной информации!)

Доступна, например, в .org;

Внедряется в .su (см. **nox.su** — подписан), ждём осенью .ru, .рф;

Требуется **поддержка** резолверами;

Неплохо может работать **вместе с другими технологиями.**

DNSSEC

Взглянем на пример внедрения: **nox.su**

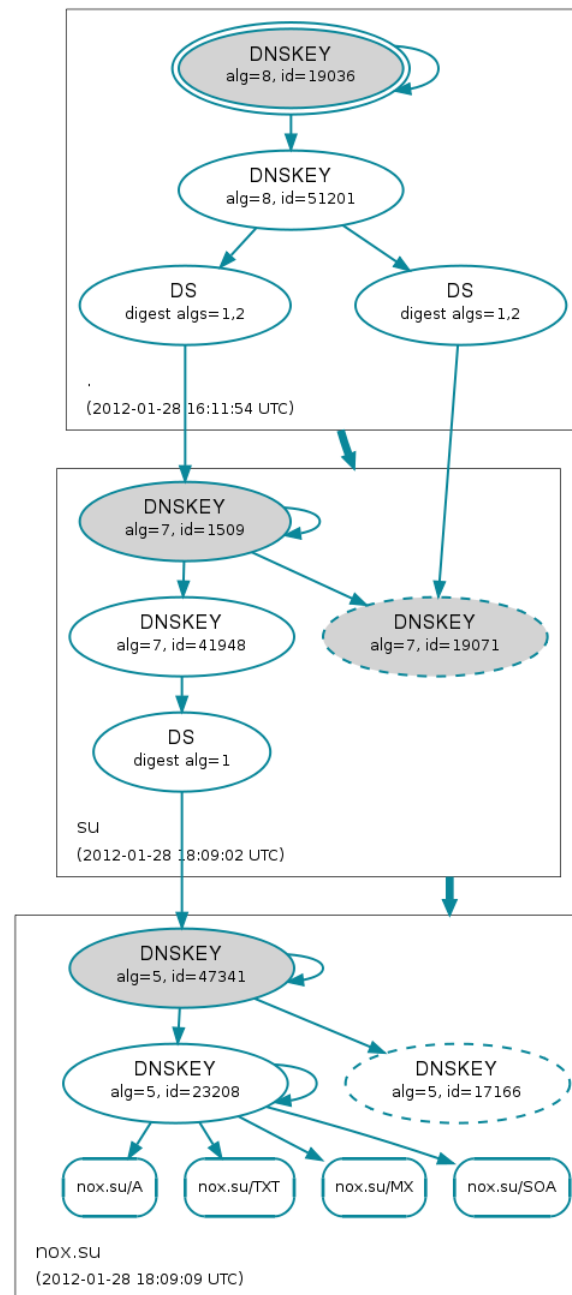
DNSSEC

Иерархическая структура

Один корень (!)

Корневой ключ - ICANN, IANA

Пример: nox.su - на картинке



SSL/TLS

Защита (потенциально) от:

- 1) подмены сайта (любым способом!);**
- 2) «прослушивания» трафика;**
- 3) изменения данных в передаваемых сообщениях.**

SSL/TLS

Выбирай на вкус:

- 1) «самоподписанный» сертификат (часто встречаются);
- 2) «полноценный» сертификат (полноценное внедрение).

Иерархия присутствует, но корней очень много (встроены в браузеры).

Практической альтернативы сейчас нет.

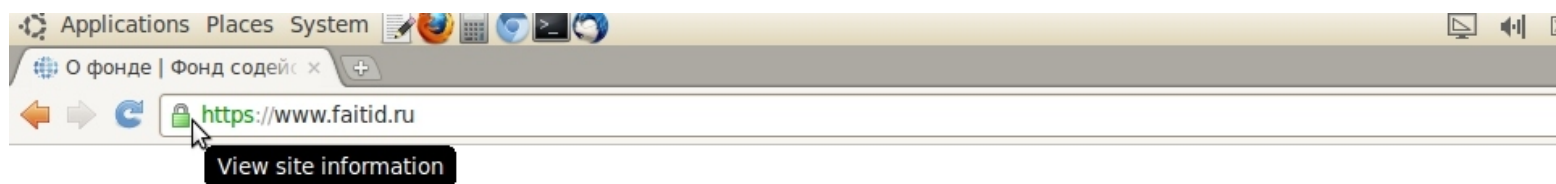
SSL/TLS

Защищает пользователей, а не сайт и его владельца.

В 2012 году
HTTPS
обязательно нужен!

SSL/TLS

Взглянем на пример внедрения: <https://www.faitid.ru/>



русский / [english](#)

+7 (495) 789-82-07

info@faitid.org

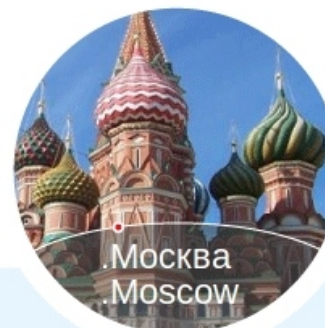


FAITID

Фонд содействия развитию технологий
и инфраструктуры Интернета



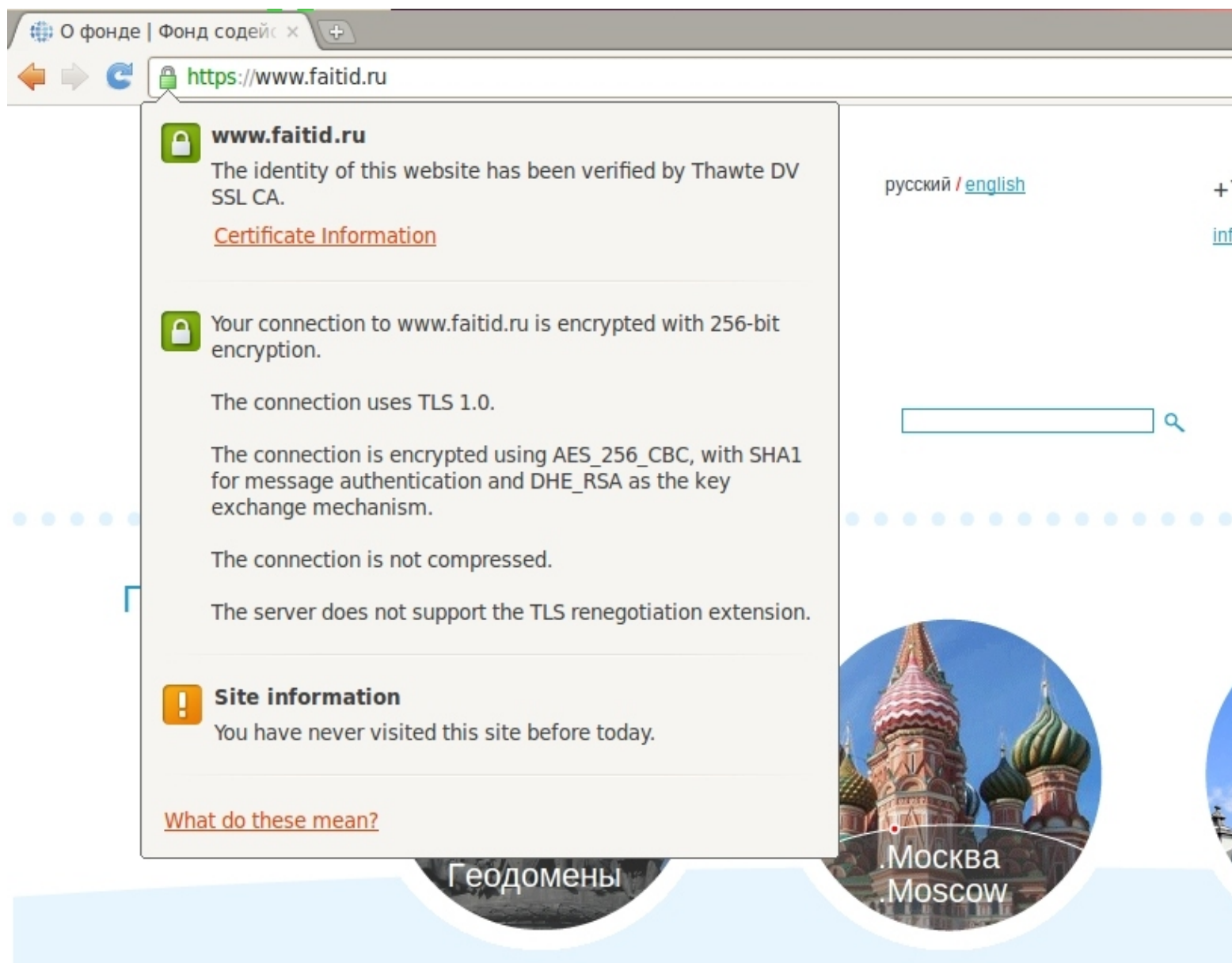
Проекты

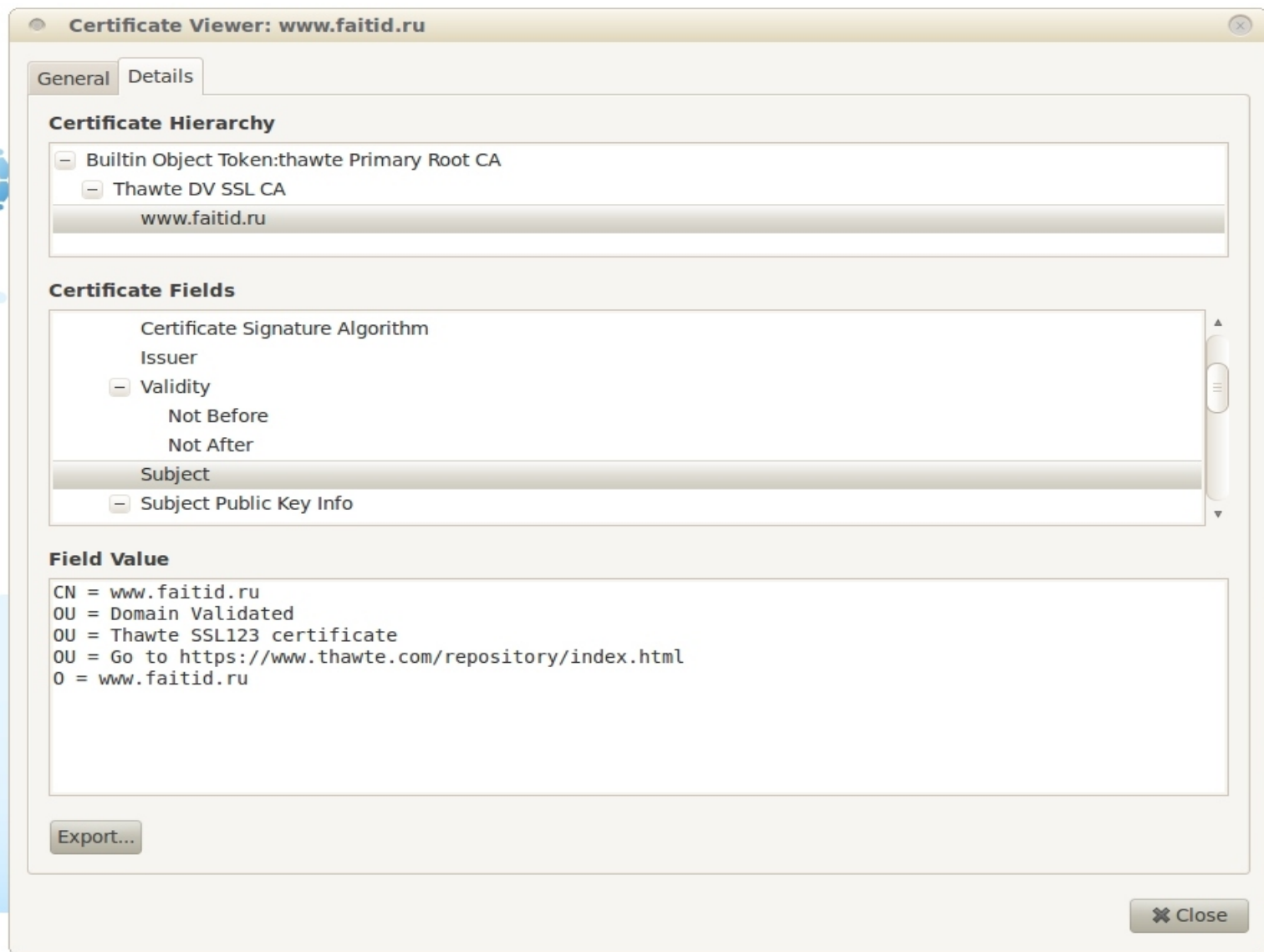


О фонде

[Состав правления](#)

Фонд содействия развитию технологий и инфраструктуры Интернета создан в 2011 году с целью осуществления системной работы с инициативами, направленными на расширение использования Интернета в интересах





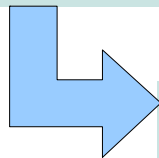
Количество подписей в поддержку

В День интернета Правительство

Подписан Меморандум о

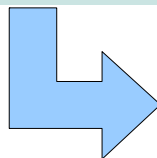
Subject
Subject Public Key Info
Field Value
CN = thawte Primary Root CA
OU = "(c) 2006 thawte, Inc. - For authorized use only"
OU = Certification Services Division
O = "thawte, Inc."
C = US

Корневой (CA) сертификат



Subject
Subject Public Key Info
Field Value
CN = Thawte DV SSL CA
OU = Domain Validated SSL
O = "Thawte, Inc."
C = US

Промежуточный сертификат



Сертификат сайта (домена)

Subject Public Key Info
Field Value
CN = www.faitid.ru
OU = Domain Validated
OU = Thawte SSL123 certificate
OU = Go to https://www.thawte.com/repository/index.html
O = www.faitid.ru

SSL/TLS

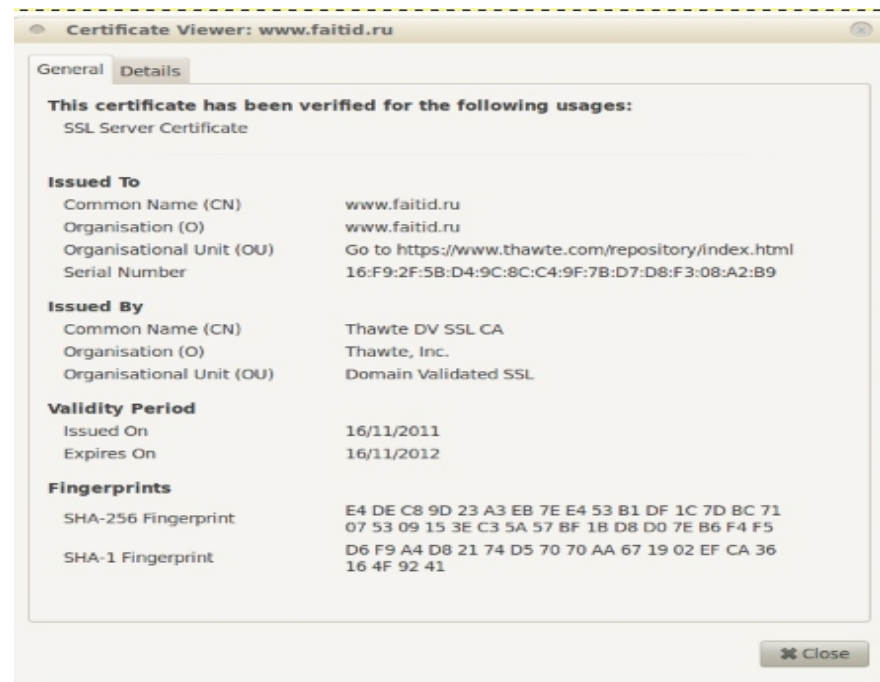
Сертификаты (для сайтов):

с проверкой домена;

с дополнительной проверкой юр. лица;

*для одного домена, для «всех»
поддоменов - *.google.com*

*для адреса e-mail, персональные,
для программ, сервисов и т. п., и т.д.*



SSL/TLS

Тезисы из практики:

рекомендуется отдельный IP-адрес для каждого веб-сервера
(но есть и поддерживается SNI - Server Name Indication);

необходимо для «админки» CMS!

необходимо для приложений в Facebook (например);

**проблема: пользователи привыкли игнорировать
предупреждения** (история с фиктивными сертификатами google.com)

Спасибо за внимание!
Вопросы?

Александр Венедюхин
dxdt.ru

Элементы и направления

