СОБИНТЕГРА

Привратник

Аутентификация в VMWare и Citrix с помощью ГОСТ’овых сертификатов

Решаемые задачи

- Привратник позволяет использовать квалифицированный сертификат ЭЦП, выданный физическому или юридическому лицу, для аутентификации в информационной системе, тем самым позволяя однозначно установить, кто именно получил доступ к информационной системе;
- Использование Привратника при доступе к информационной системе организации позволяет переложить юридические риски в случае утечки информации на то юридическое или физическое лицо, чей квалицированный сертификат был использован при аутентификации;
- При использовании данного решения, факт аутентификации в ИС становится юридически значимым, следовательно все действия совершённые после аутентификации с помощью квалифицированного сертификата расцениваются как совершённые лицом, которому был выдан квалифицированный сертификат принадлежит;
- При аттестации информационной системы, для работы с персональными данными и соответствии ФЗ 152, использование сертифицированного решения Привратник будет являться преимуществом;
- Привратник может быть использован как наложенное средство аутентификации по ГОСТ’овым сертификатам;

Типы сотрудников и сценарии работы

- Сценарии работы:
  - Работа с «критичными» данными при доступе внутри организации;
  - Удалённый сотрудник организации, который обрабатывает персональные данные клиентов;
- Внутренние сотрудники - требуется дополнительная аутентификация к «критически важным» (не только персональным) данным изнутри ИС:
  - Медицинские учреждения;
  - Компании с гос. участием;
  - Государственные структуры;
- Сотрудники подключающиеся удалённо – удалённые офисы, удалённые точки присутствия, мобильные сотрудники «в полях»:
  - Банковский сектор;
  - Страховые компании;
  - Телекоммуникационные компании;
- Агенты/контрагенты – другое юридическое лицо, работающее по договору и получающее доступ к «критически важным» (не только персональным) данным организации:
  - Страховые компании;
  - Телекоммуникационные компании;

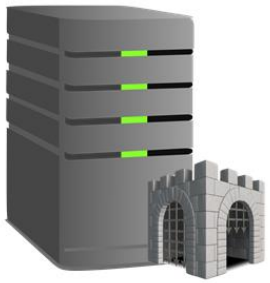
Привратник с Citrix

- Аутентификация по ГОСТ’овым сертификатам в инфраструктуре Citrix:

NetScaler

StoreFront 3.9

+

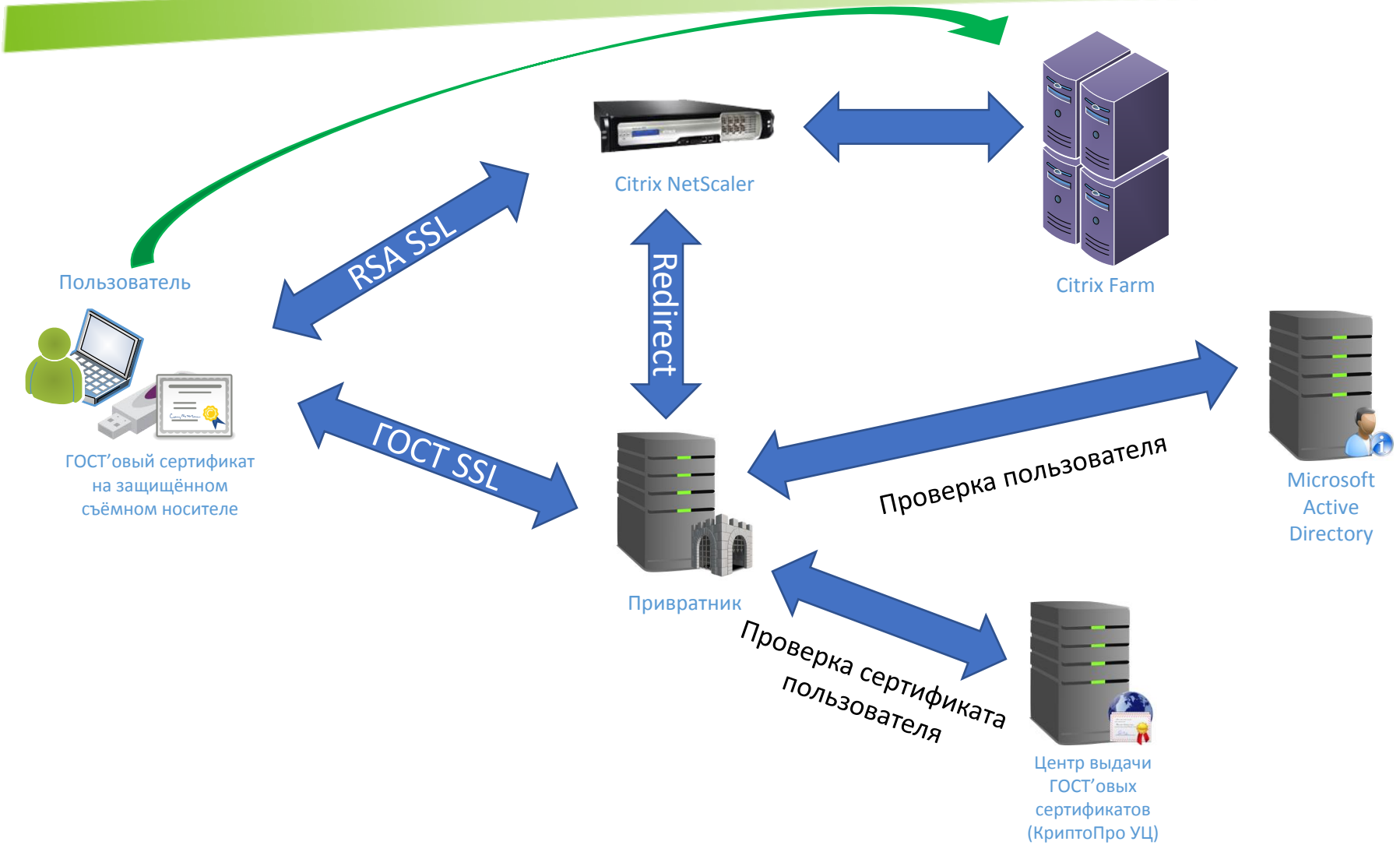


Привратник

=

Аутентификация по ГОСТ’овым сертификатам

Привратник – Схема работы с Citrix.



1. IE: Установка RSA-SSL соединения с Citrix NetScaler и HTTP редирект на Привратник;
2. IE: Установка ГОСТ-SSL соединения с Привратником на ГОСТ сертификате пользователя
3. Привратник: Проверка пользователя в Active Directory по его ГОСТ сертификату
4. Привратник: Ответ HTTP содержащий SAML assertion, который редиректится на NetScaler
5. NetScaler: Обработка assertion и допуск пользователя к веб-странице с каталогом рабочих столов и приложений

Требования к инфраструктуре Citrix

- Удостоверяющий Центр, выдающий ГОСТ’овые сертификаты;
- Привратник;
- NetScaler Gateway 11.0 и выше + StoreFront 3.6 и выше
  или StoreFront 3.9 без NetScaler;
- Citrix Federated Authentication Service;
- XenApp/XenDesktop;
- Крипто провайдер на клиентском ПК + отчуждаемый ключевой носитель;

Привратник с VMWare

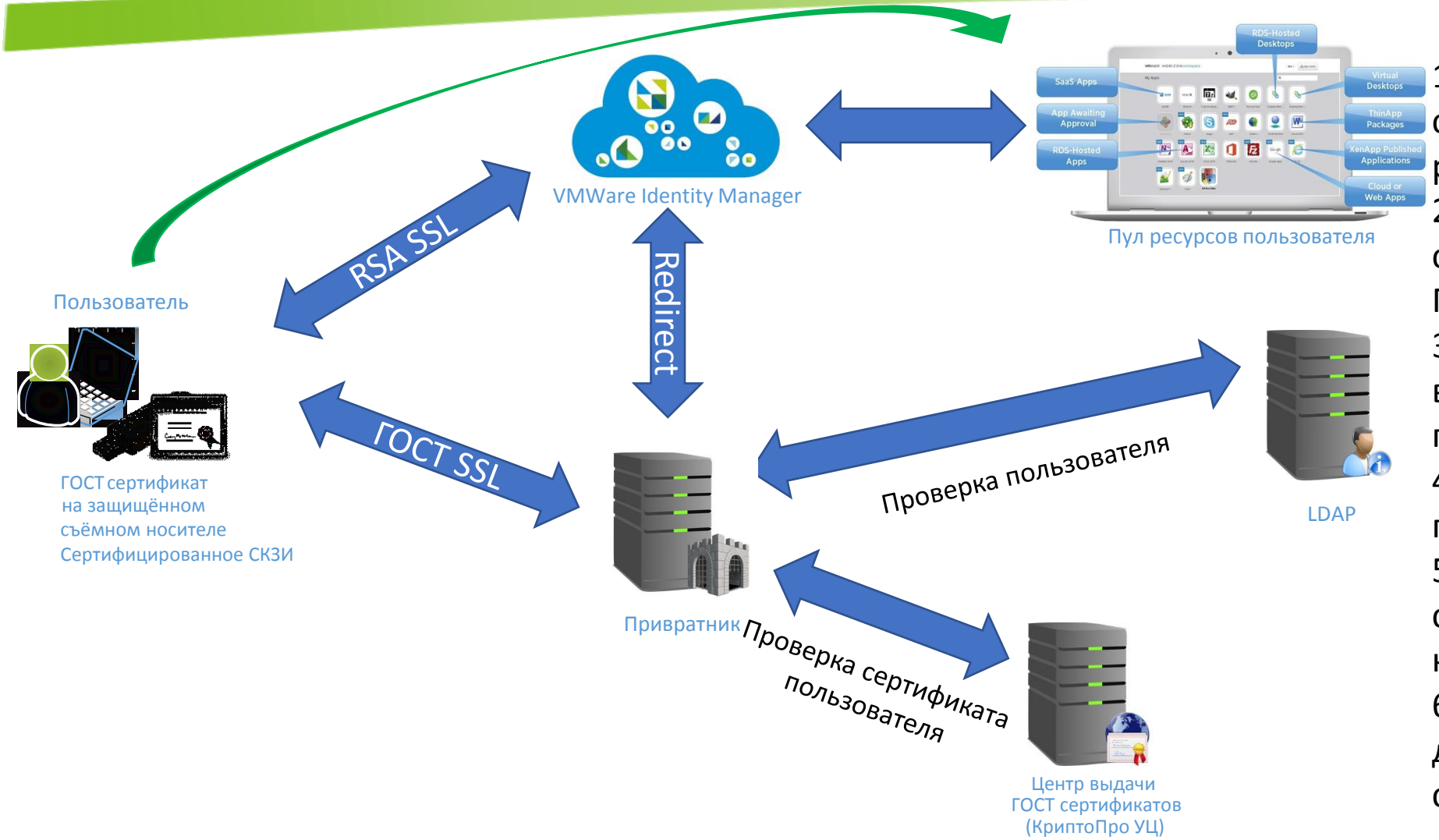
- Аутентификация VMWare с использованием цифровых сертификатов ГОСТ и сертифицированных СКЗИ:

VMWare Identity Manager

Привратник

Аутентификация по ГОСТ сертификатам

Привратник – схема работы с VMWare.



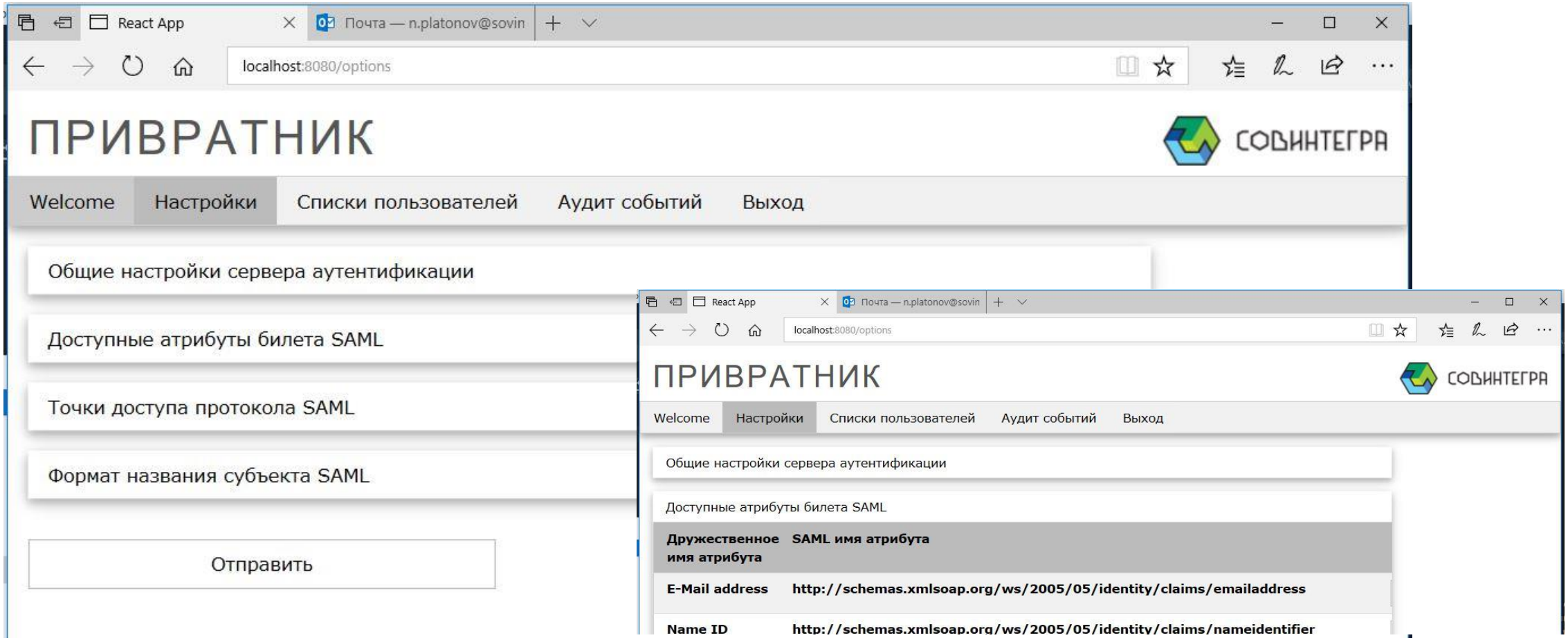
1. IE: Установка RSA-SSL соединения с Idm, HTTP(S) редирект на Привратник;
2. IE: Установка ГОСТ-SSL соединения с Привратником на ГОСТ сертификате пользователя
3. Привратник: Проверка валидности сертификата пользователя
4. Привратник: Проверка пользователя в Active Directory
5. Привратник: Ответ HTTP(S) содержащий SAML assertion, который возвращается на Idm
6. Idm: Обработка assertion и допуск пользователя к веб-странице с каталогом ресурсов

Требования к инфраструктуре VMWare

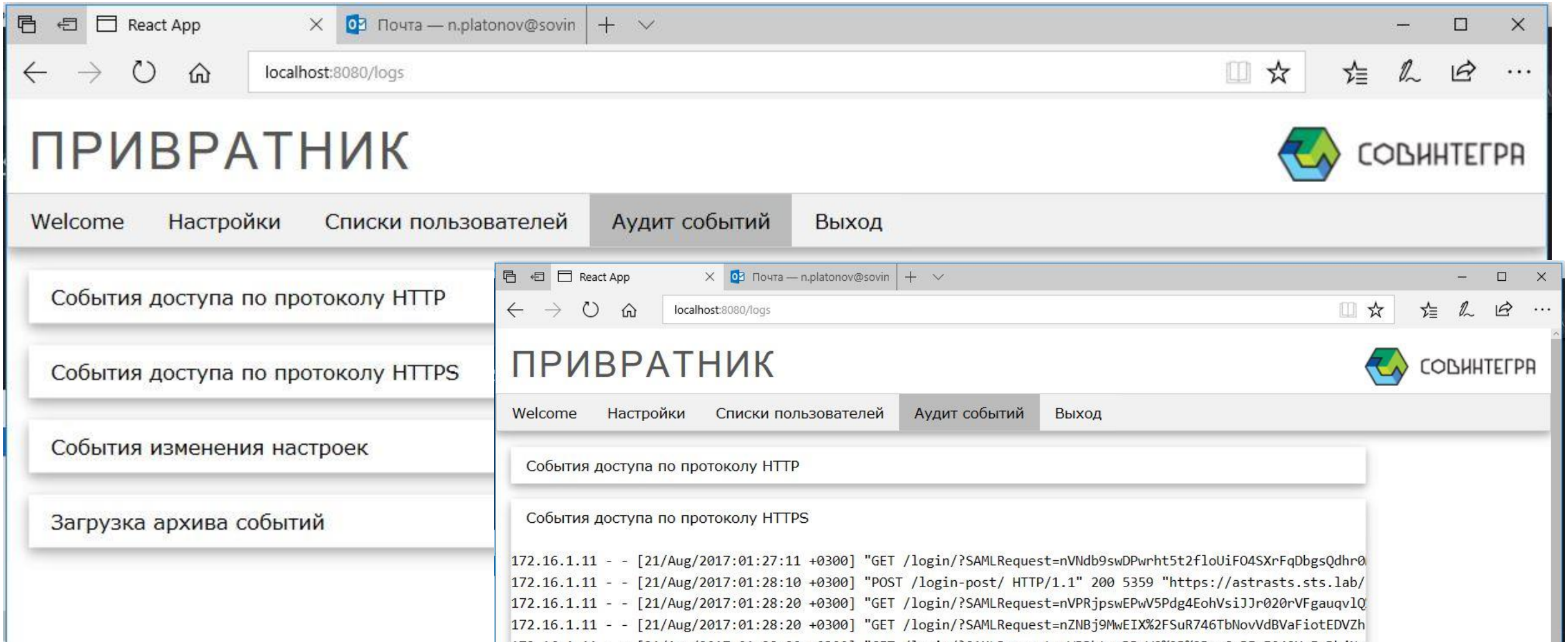
- Удостоверяющий Центр, выпускающий ГОСТ сертификаты;
- Привратник;
- VmWare Identity Manager 2.8
  или Horizon 7.02 и выше;
- Криптопровайдер на клиентском ПК + отчуждаемый ключевой носитель;

Интерфейс Привратника

- Web-интерфейс для настройки и работы с Привратником

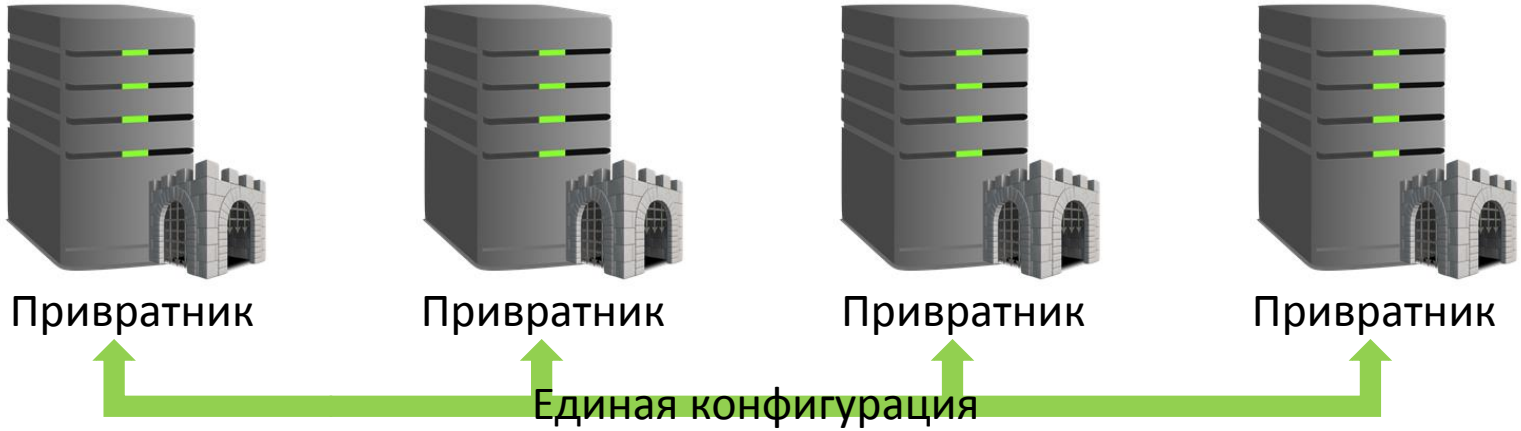


Аудит событий



Отказоустойчивость и балансировка нагрузки

- Для обеспечения отказоустойчивости и балансировки нагрузки предлагается использоваться несколько Привратников, объединённых в «роту»:



Рота Привратников на страже доступа к Вашей информационной системы

Привратник – возможности

SAML

Security Assertion Markup Language

CITRIX И ДРУГИЕ...

Лицензирование

- Лицензирование по пользователю, независимо от количества серверов в «роте»;
- Привратник доступен в двух конфигурациях:

Аппаратный привратник

Виртуальный привратник

Лицензирование

- Базовая лицензия является срочной и включает в себя техническое сопровождение решения и получение обновлений.
- Лицензии приобретаются диапазонами:
  - 100 пользователей;
  - 500 пользователей;
  - 1 000 пользователей;
  - 2 500 пользователей;
  - 5 000 пользователей;
  - 10 000 пользователей
  - Свыше 10 000 пользователей;

Сертификация

- Поданы на сертификацию во ФСТЭК:
  - Сертификация по ТУ;
  - Сертификация на НДВ;
- Сертификация ФСБ не требуется

История успеха

- Совместный вебинар с компанией Citrix о создании комплексного решения для удалённого доступа с аутентификацией по ГОСТ’овым сертифкатам;
- Успешный пилотный проект в одном из крупных сотовых телекоммуникационных компаний:
  - Удалённый доступ сотрудников к приложениям и рабочим столам, развёрнутым на VMWare с аутентификацией по ГОСТ’овым сертификатам, расположенным на смарт-картах;

Планы развития

- Ближайшие планы
  - Реализация механизма чёрных и белых списков;
- Стратегия развития
  - Реализация поддержки стандарта OpenID;
  - Интеграция с решениями защиты сетевых каналов;

О компании

СОВИНТЕГРА – молодая развивающаяся технологическая компания:

- Поставщик решений по информационной безопасности и ИТ решений;
- Разработчик собственных решений в области аутентификации и информационной безопасности;
- Технологический партнёр компании Gemalto – мирового лидера решений по аутентификации и информационной безопасности;
- Большой успешный опыт проектов по информационной безопасности в следующих отраслях:
  - Нефтегазодобывающие компании;
  - Банки;
  - Телекоммуникационные компании;
  - Фармакологические компании;

О людях

Роман Совалов – *генеральный директор.* В ИТ более 15 лет. Работал в системных интеграторах, поднялся с инженерных позиций до руководителя проектного отдела. За плечами опыт работы в Microsoft Consulting Services. Принимал участие в разработке системы Платон. Имеется опыт работы в крупномасштабных проектах;

Сергей Алимпиев – *директор по развитию бизнеса.* В ИТ более 20 лет. Работал в заказчиках и вендорах – знает потребности и особенности работы с обеих сторон. Руководил техническими подразделениями и выстраивал процессы работы ИТ подразделений в крупных компаниях.

Сергей Грибков – *технический директор.* В ИТ более 15 лет. Работал и со стороны заказчиков, интеграторов и вендоров, знает ИТ процессы от создания продукта до его эксплуатации. Руководил командами эксплуатации и внедрения ИТ решений.

Николай Платонов – *руководитель разработки.* В ИТ более 15 лет. Гуру разработки решений для информационной безопасности и аутентификации в частности. Работал в одном из передовых поставщиков решений на рынке ИБ в России. Проходил обучение в компании Gemalto.

Спасибо за Ваше внимание.

Ждём Ваши вопросы на privratnik@sovintegra.ru