Осторожно!
Server Side Signature

Алексей Уривский, Алексей Качалин

ОАО «ИнфоТеКС»
urivskiy@infotecs.ru; kachalinai@infotecs.ru

ViPNet® Virtual Private Network

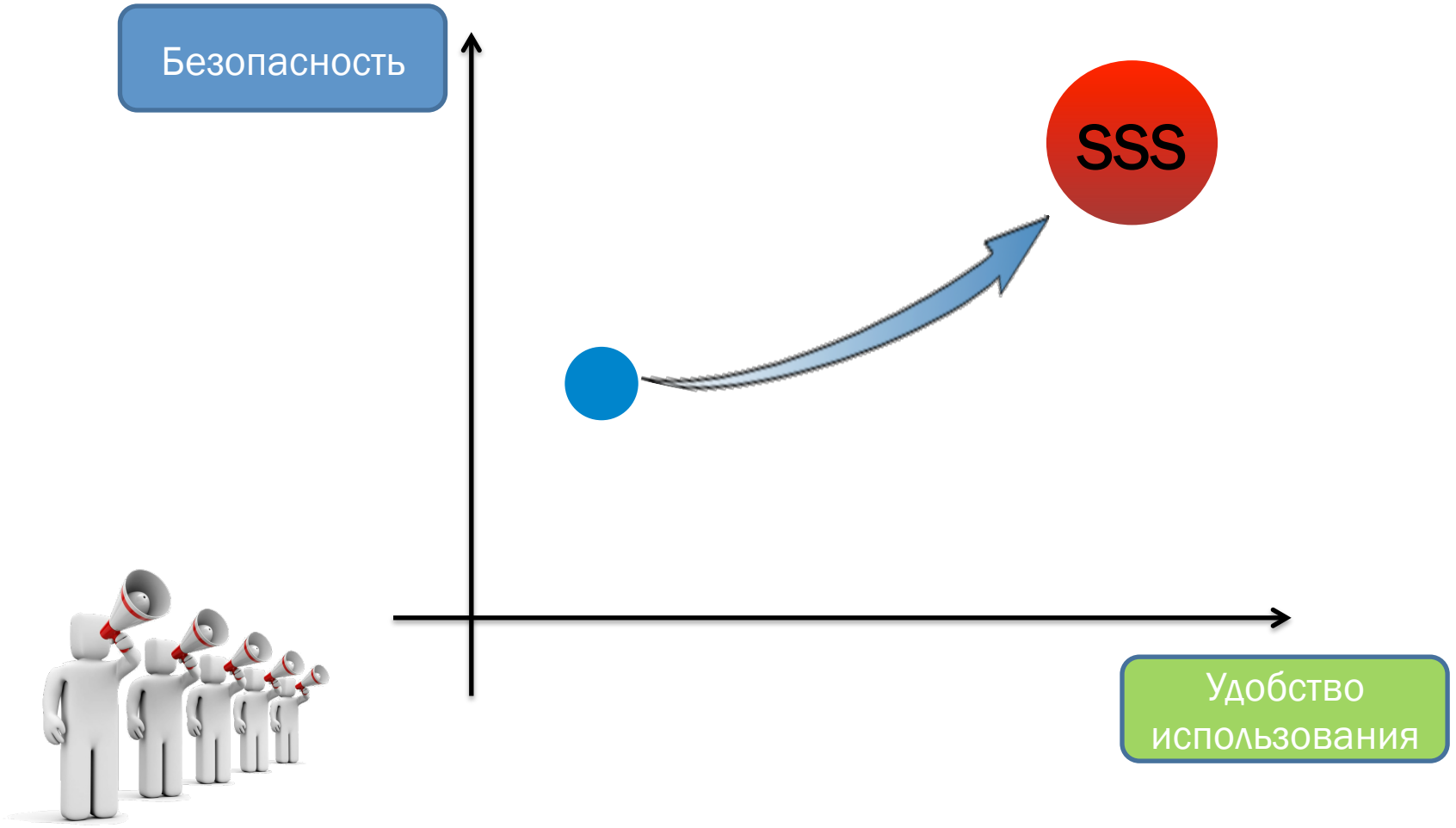
infotecs®

Альтернативы по средствам ЭП

- Криптопровайдеры
- TPM (trusted platform module)
- Аппаратные криптографические токены – smart-карты, USB-токены
- SIM-карты
- **Server Side Signature – централизованная подпись на сервере**

Типичная схема SSS

Агитация за Server Side Signature



«Неудобства» традиционных пользовательских средств ЭП

- ЭП на рабочем месте пользователя
  - Низкая квалификация пользователя
  - Сложное управление
  - Злоупотребления
- Программное и аппаратное окружение средств ЭП
  - Статический список средств
  - Низкая мобильность
- Требования к сертифицированным средствам ЭП
  - Хранение и учет
  - Правила эксплуатации

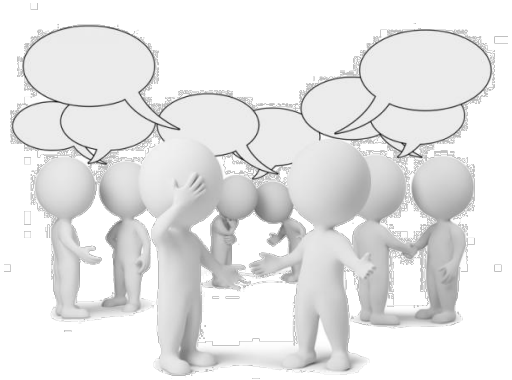
Повышение удобства / безопасности?

- Удобство
  - Удобство развертывания и администрирования системы
  - Централизованные политики безопасности
  - Поддержка мобильных платформ
  - Отсутствие пользовательской криптографии
- Безопасность
  - Серверный аппаратный криптомодуль (HSM) для хранения ключей и формирования подписи
  - Удаленная двухфакторная аутентификация пользователей и запросов на подпись

Пользователь с удобным мобильным устройством

- **Канал взаимодействия с сервером**
  - Защита канала TLS/SSL протоколом: пользовательская криптография
  - Недостаточная длина ключей на маломощных устройствах
  - Подмена браузера и сторонние сборки
  - Вирусный перехват SSL-сессии (SSL Hijacking)
- **Доверие к PKI**
  - Источник корневых сертификатов:
    вендор браузера на свое усмотрение размещает корневые сертификаты
  - Доверие к публичным УЦ: поддельные серверные сертификаты (DigiNotar, Comodo)
  - Подлинность корневых сертификатов: вирус подменяет корневой сертификат
  - Параметры сертификатов: короткие ключи / нестойкие хэш-функции
- **OTP** через SMS
  - Канал доставки OTP совпадает с каналом подтверждения
  - Вирусная активность
  - Фишинговые сайты
- **Разбор конфликтных ситуаций**
  - Не менее трех участников процесса
  - Разграничение ответственности
  - Материальное обеспечение/страхование ответственности

Ожидаемое развитие ситуации



X ежегодная международная конференция
«PKI-ФОРУМ РОССИЯ 2012»

Спасибо за внимание!
Вопросы?

Алексей Уривский, Алексей Качалин
ОАО «ИнфоТеКС»
urivskiy@infotecs.ru