ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСТИТЕТ

ГЛАВНЫЙ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ
ВЫЧИСЛИТЕЛЬНЫЙ ЦЕНТР

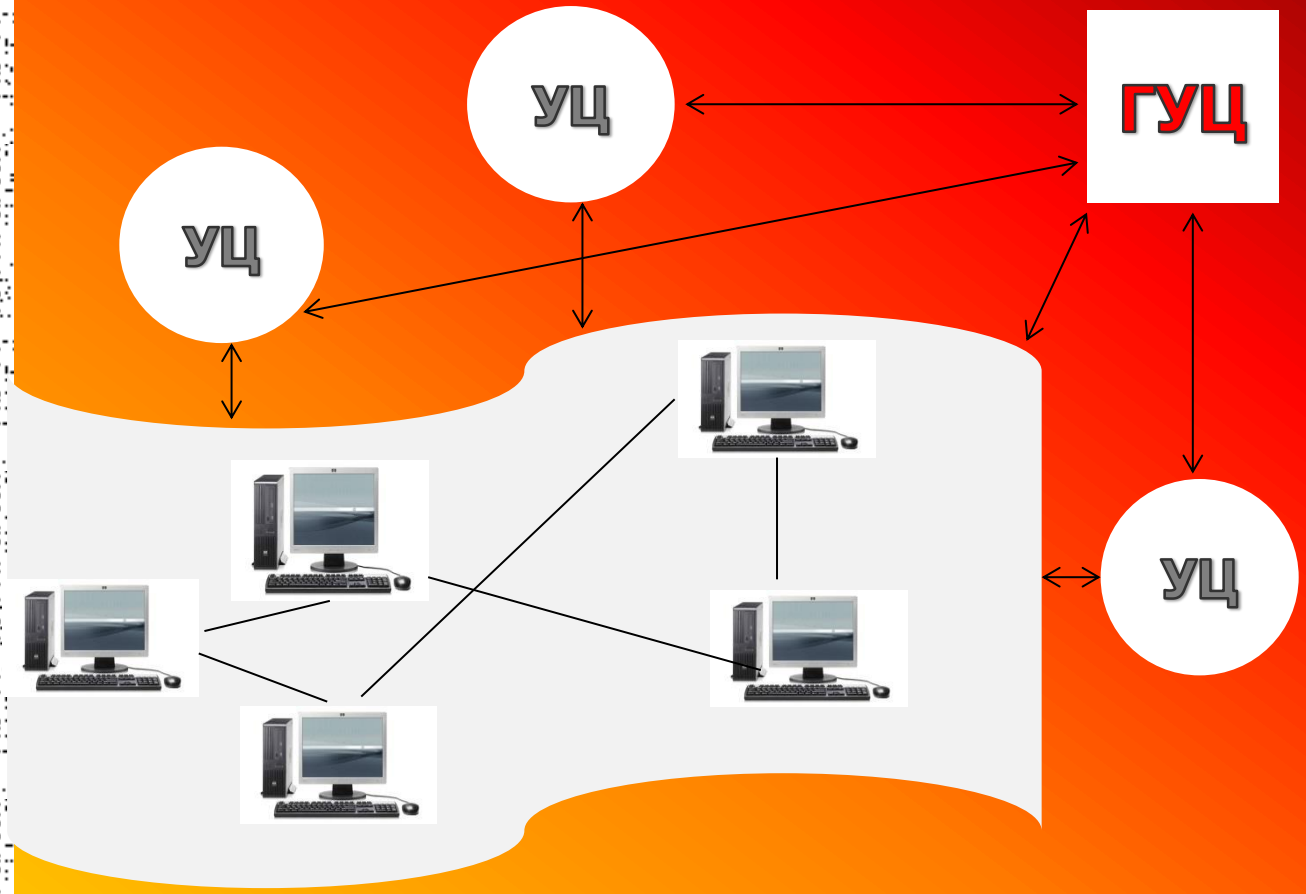
ПРОБЛЕМЫ МАССОВОГО ПРИМЕНЕНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ (ЭП)

АКАДЕМИК АКАДЕМИИ КРИПТОГРАФИИ
А.П. БАРАНОВ

ОСОБЕННОСТИ НЕ ПРОСТОЙ ЭП У ПОЛЬЗОВАТЕЛЯ

- Биометрическая характеристика личности заменяется на цифровой публичный идентификатор – сертификат ключа ЭП (СКЭП) и личный конфиденциальный идентификатор – ключ ЭП (КЭП)
- КЭП и СКЭП – применяются в течении длительного времени. СКЭП есть следствие КЭП, а КЭП необходимо сохранить в тайном электронном виде
- Для реализации усиленной ЭП необходимо специальное пользовательское ПО. Для квалифицированной усиленной ЭП (КУЭП) реализация специализированного ПО должна быть сертифицирована с ограничениями по базовым операционным системам (ОС)
- Следствие. Пользователь должен иметь не тривиальную квалификацию и определенный (по возможности минимальный) материальный ресурс (стоимость носителя КЭП, СКЭП, легальная ОС, сертифицированное легальное ПО)

СХЕМА МАССОВОГО ВЗАИМОДЕЙСТВИЯ



- В облаке – полный граф взаимодействия пользователей
- В облаке привязанные к УЦ "облака"

ОСОБЕННОСТИ ВЗАИМОДЕЙСТВИЯ ПРИ РЕАЛИЗАЦИИ КУЭП

- При взаимодействии пользователя (подписанта) и проверяющего (получателя) вместе с ЭП используется SSL на базе СКЭП. Следовательно, проверяющий должен иметь несколько вариантов специального ПО
- УЦ должен обеспечивать гарантированный доступ в режиме 24 х 7 для обеспечения проверки валидности СКЭП
- При изменении СКЭП и специализированного ПО вследствие изменений Закона или действий регуляторов (1024 → 2048), организация своевременной замены СКЭП у всех УЦ и пользователей
- ГУЦ – главный удостоверяющий центр. Поддержка и регулярное обновление списка отозванных сертификатов. Публичный регламент деятельности, высокая телекоммуникационная доступность

ПРОБЛЕМЫ ОСНОВНОЙ МАССЫ ПОЛЬЗОВАТЕЛЕЙ МАЛОЙ СОБСТВЕННОЙ ЗАГРУЗКИ (ПМЗ) (I)

- ПМЗ – зарегистрировано более 10^7, при их работе происходит взаимодействие с небольшим числом других пользователей и УЦ
- Аутентификации и выдачи КЭП и СКЭП для 10^7 ПМЗ – проблема личного посещения и общей стоимости выдачи КЭП на носителе (более 10^9 рублей)
- Решение: Аутентификация с явкой в орган выдачи личного пароля, отдельно от вырабатываемого самостоятельно КЭП, с передачей открытого ключа в УЦ для выработки СКЭП с подтверждением личным паролем, зашифрованным на КЭП
- Необходим персональный криптопровайдер: удобный для большого числа базовых ОС, сертифицированный и бесплатный
- Проблема длительного хранения в тайне КЭП может быть решена его регулярной заменой с выдачей набора паролей аутентификации. Возрастает роль Списка отозванных сертификатов

ПРОБЛЕМЫ ПМЗ (II)

- УЦ независимо от юрисдикции владельца должны нести одинаковую, реальную юридическую и финансовую ответственность, что в Российской практике для 300 УЦ невозможно. Выход: сокращение числа УЦ – ликвидация выданных лицензий, как ЦБ
- УЦ и аутентификационный орган должны быть технически и юридически сопряжены, неся солидарную ответственность
- Число видов криптопровайдеров и SSL должно быть два – три, тогда у ПМЗ большая свобода взаимодействия
- Массовая замена СКЭП будет требовать специальных решений. 10^6 СКЭП меняли 2 года

ОСОБЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ БОЛЬШОЙ ЗАГРУЗКИ (ПБЗ)

- ПБЗ порядка 10^4, взаимодействие с не более 10^3 пользователей (крупные фирмы с филиалами и малым числом постоянных корреспондентов, около 100)
- Аутентификация и хранение ключей решаются организационными мерами
- Специальное ПО ограничивается одним – двумя вариантами
- ПБЗ – мало проверяют ЭП, они сами рассылают большое число электронных документов (ЭД) с ЭП
- Замена ПО и СКЭП не представляет проблемы, хватает 0,5 года

ПРОБЛЕМА ПОЛЬЗОВАТЕЛЕЙ СВЕРХБОЛЬШОЙ ЗАГРУЗКИ (ПСБЗ)

- ПСБЗ – порядка 10^3 , крупные операторы ЭДО (ОЭДО), Интернет- магазины, банки, сайты, реализующие личные кабинеты (ЛК) и взаимодействующие с 10^7 ПМЗ
- Собственная аутентификация и хранение ключей решаются эффективно
- Разные ПМЗ требуют специальное ПО различных производителей, включая SSL. Необходима библиотека сертифицированного специального ПО по реализации ЭП и SSL
- Основная масса ОЭДО обслуживает клиентов на собственном УЦ и для них реализует проверку ЭП эффективно. Для ЛК государственных ведомств такая технология неприемлема. Требуется On-line взаимодействие со всеми УЦ в режиме 24 х 7
- При обслуживании ЛК возрастает роль ГУЦ. Необходима централизованная поддержка и регулярная актуализация Списка отозванных сертификатов

В Ы В О Д Ы

- Массовое применение ЭП требует жесткого, эффективного и ответственного регулирования отрасли
- Как УЦ, так и регуляторы должны нести юридическую и финансовую ответственность за невыполнение установленных публичных регламентов
- Требования по доступности и надежности работы УЦ, включая ГУЦ, должны сопровождаться законодательными, компенсационными мерами, включая штрафами установленных размеров
- Взаимодействие Минкомсвязи России, ФСБ России и пользователей ЭП в области законодательных инициатив и выработке регулирующих воздействий оставляет желать лучшего
- Постоянный Консультативный совет по ЭП с участием ПСБЗ, регуляторов и заинтересованных ведомств был бы полезен.


СПАСИБО
ЗА ВНИМАНИЕ