Ежегодная международная научно-практическая конференция
«РусКрипто’2019»

Аспекты безопасности решений на основе распределенного реестра в свете российских требований

Багин Дмитрий,
Зам.начальника отдела анализа безопасности систем,
ООО «КРИПТО-ПРО»

Нормативные документы

- Требования ФСБ России к СКЗИ или Рекомендации по стандартизации Р 1323565.1.012-2017 «Принципы разработки и модернизации шифровальных…»
- Федеральный закон «Об электронной подписи» № 63-ФЗ (и соответствующие Требования ФСБ России к средствам ЭП)

Вопросы при сертификации блокчейн-решений

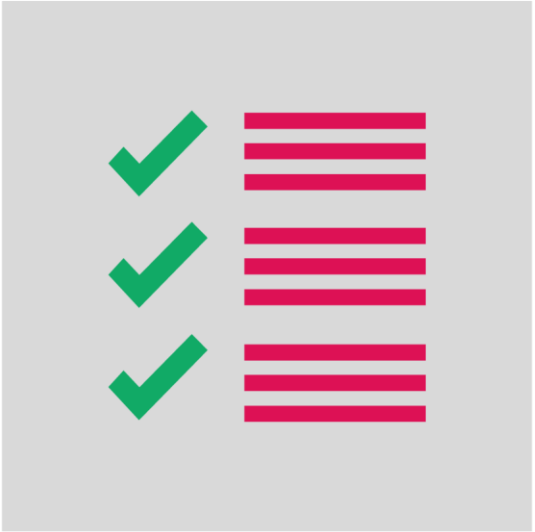
- Используемые алгоритмы
- Обеспечение защиты от НСД
- Работа с ключевой информацией
- Создание/проверка ЭП
- Работа с конфиденциальными данными

Используемые алгоритмы

- «Короткие» хэши
- Модифицированные алгоритмы (например, формирования/проверки ЭП)

Обеспечение защиты от НСД. Вопросы

- Идентификация/аутентификация пользователей
- Контроль целостности

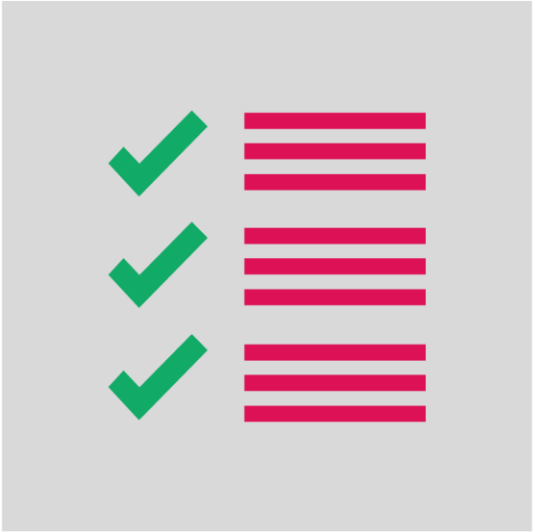


Обеспечение защиты от НСД. Решение

- Аутентификация
  - ГОСТовый TLS для аутентификации пользователя и защиты доступа к узлу
  - ГОСТовый TLS для защиты канала между узлами
- Дополнительное назначение ключа в сертификате + ролевая модель
- Контроль целостности за счет встроенных механизмов КриптоПро

Ключевая информация. Вопросы

- Срок действия ключей
- Разделение ключей по назначению
- Защита ключей при эксплуатации

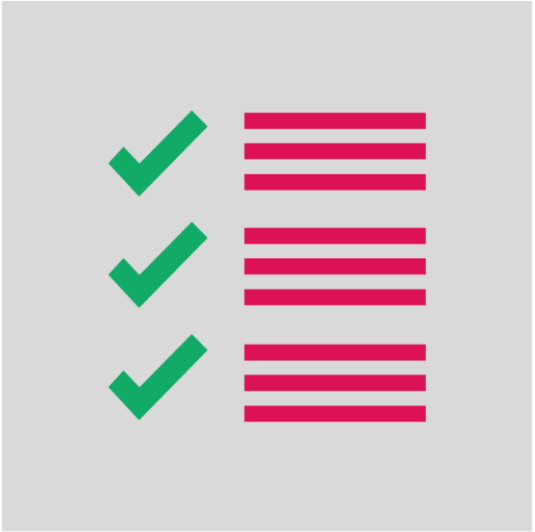


Ключевая информация. Решение

- Работа с ключами средствами КриптоПро
- Сроки действия ключей:
  - Закрытый ключ (ключ ЭП) - 1 год 3 месяца
  - Открытый ключ (ключ проверки ЭП) - 15 лет
- Использование различных ключей для каждой криптографической операции

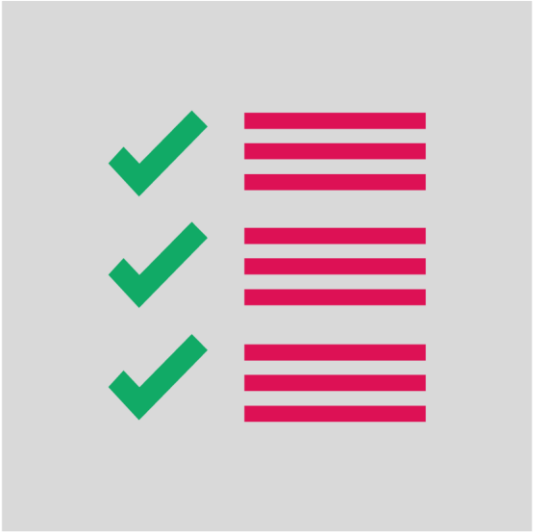
Создание/проверка ЭП. Вопросы

- Требования к алгоритмам
- Требования к процедурам формирования и проверки ЭП
- Требования к работе с УЦ



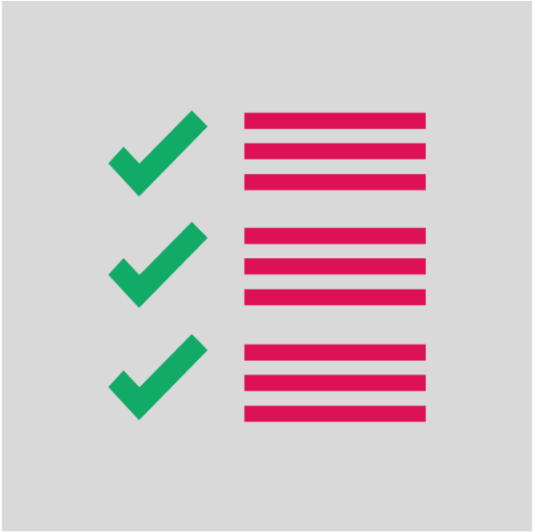
Квалифицированная и не квалифицированная ЭП. Решение

- Сертификаты издаются выделенным УЦ
- При создании/проверке ЭП реализованы указанные требования к отображению



Работа с конфиденциальными данными. Вопросы

- Возможность работы с конфиденциальными данными (данными ограниченного доступа)
- Обеспечение ролевого доступа



Работа с конфиденциальными данными. Решение

- В блокчейне сохраняется «слепок» документа
- Ролевой доступ к данным (в блокчейне также сохраняется информация о правах доступа)

Вопросы

Контактная информация

Электронная почта:

Bagin.dmitry@cryptopro.ru

Телефон:

+7 985 206-06-95

Facebook:

facebook.com/cryptopro

Сайт:

www.cryptopro.ru