Вопросы использования ключей в системах юридически значимого электронного документооборота

ООО «КРИПТО-ПРО»
коммерческий директор
Маслов Юрий Геннадьевич
maslov@cryptopro.ru

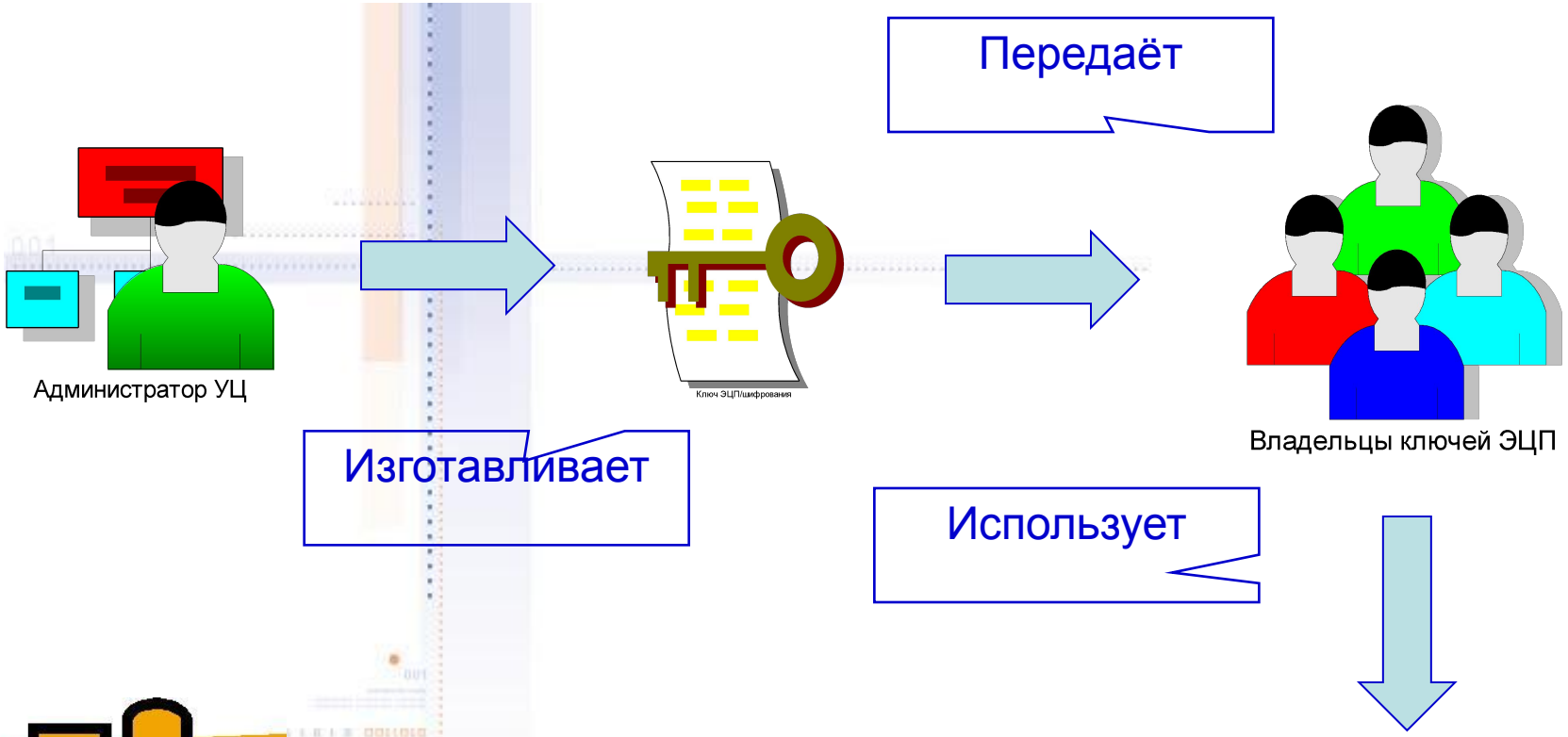
«И опыт - сын ошибок трудных»

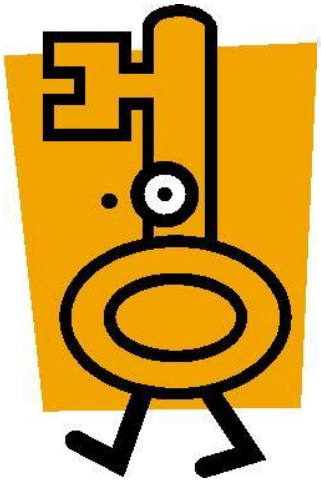
А.С. Пушкин

Основания, что бы прислушаться:

1. Объем продаж ПАК «КриптоПро УЦ»: свыше 750 копий
2. Объем продаж СКЗИ КриптоПро CSP: свыше 2 млн 600 тысяч копий
3. ООО «КРИПТО-ПРО» и ее сотрудники принимали участие в 16 инцидентах, которые разрешались в судебном и/или в досудебном порядке или находились в производстве у дознавателя (следователя).

Традиционный подход хранения и использования ключей





- Ключи хранятся на съёмных носителях;
- Находятся во владении пользователей;
- Пользователи сами обеспечивают сохранность

Жизнь задаёт свои вопросы

Какие вопросы могут возникнуть при применении ЭЦП и шифрования, связанные с закрытыми ключами и ключевыми носителями?

1. Могло ли получить постороннее лицо доступ к закрытому ключу?
2. Как расшифровать данные в случае утраты или порчи ключевого носителя с закрытым ключом?
3. Какие меры нужно предпринять для предотвращения случайной утери ключевого носителя?
4. Как надежно предотвратить возможность случайного или преднамеренного копирования закрытого ключа?

А если не отвечать на вопросы?

Способы отказа от ЭЦП

«Сломать» ГОСТы

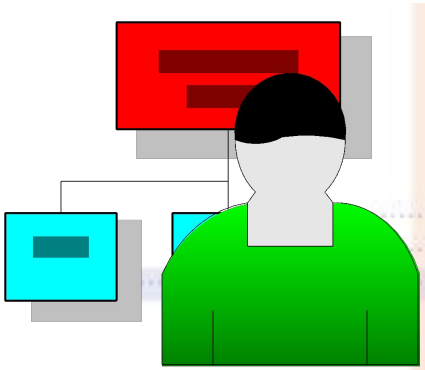
«Сломать» УЦ

Отказаться от сертификата

Похитить ключ ЭЦП

Предположить, что постороннее лицо получило или могло получить доступ к закрытому ключу

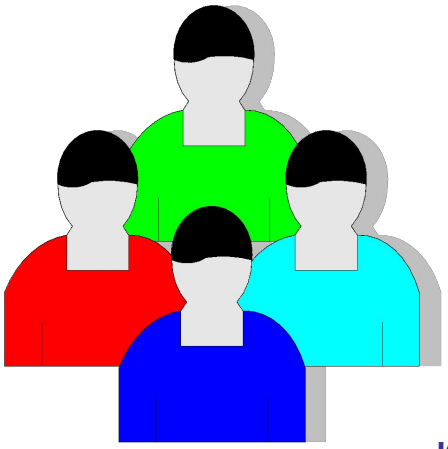
Есть ответ !!!



Администратор УЦ

Изготавливает

Использует



Владельцы ключей ЭЦП

КОМПАНИЯ КРИПТО-ПРО
ключевое слово в защите информации
www.cryptopro.ru

ПАКМ «Атликс HSM» версии 2.0

- «Атликс-HSM» внутри себя реализует криптографические алгоритмы шифрования и формирования ЭЦП;
- Ключи пользователей формируются внутри устройства и никогда не покидают его;
- На рабочих местах пользователей стоит псевдо криптопровайдер («Атликс CSP»), который выполняет только криптографические преобразования не связанные с использованием закрытых ключей и обеспечивает канал и аутентификацию пользователей с устройством для доступа к личным ключам;
- Доступ к ключам осуществляется по защищенному (шифрованному) каналу;
- Аутентификация осуществляется как по ключам и сертификату аутентификации (строгая аутентификация), так и по логин-паролю (не строгая аутентификация).

ВОПРОСЫ?

Маслов Юрий Геннадьевич

maslov@cryptopro.ru