конференция
РусКрипто'2010

Особенности реализации прозрачного шифрования файлов в КриптоПро EFS

ООО «КРИПТО-ПРО»
ведущий специалист, к.т.н
Смирнов Павел
spv@cryptopro.ru

КОМПАНИЯ КРИПТО-ПРО
КЛЮЧЕВОЕ СЛОВО В ЗАЩИТЕ ИНФОРМАЦИИ
WWW.CRYPTOPRO.RU

Что такое EFS?

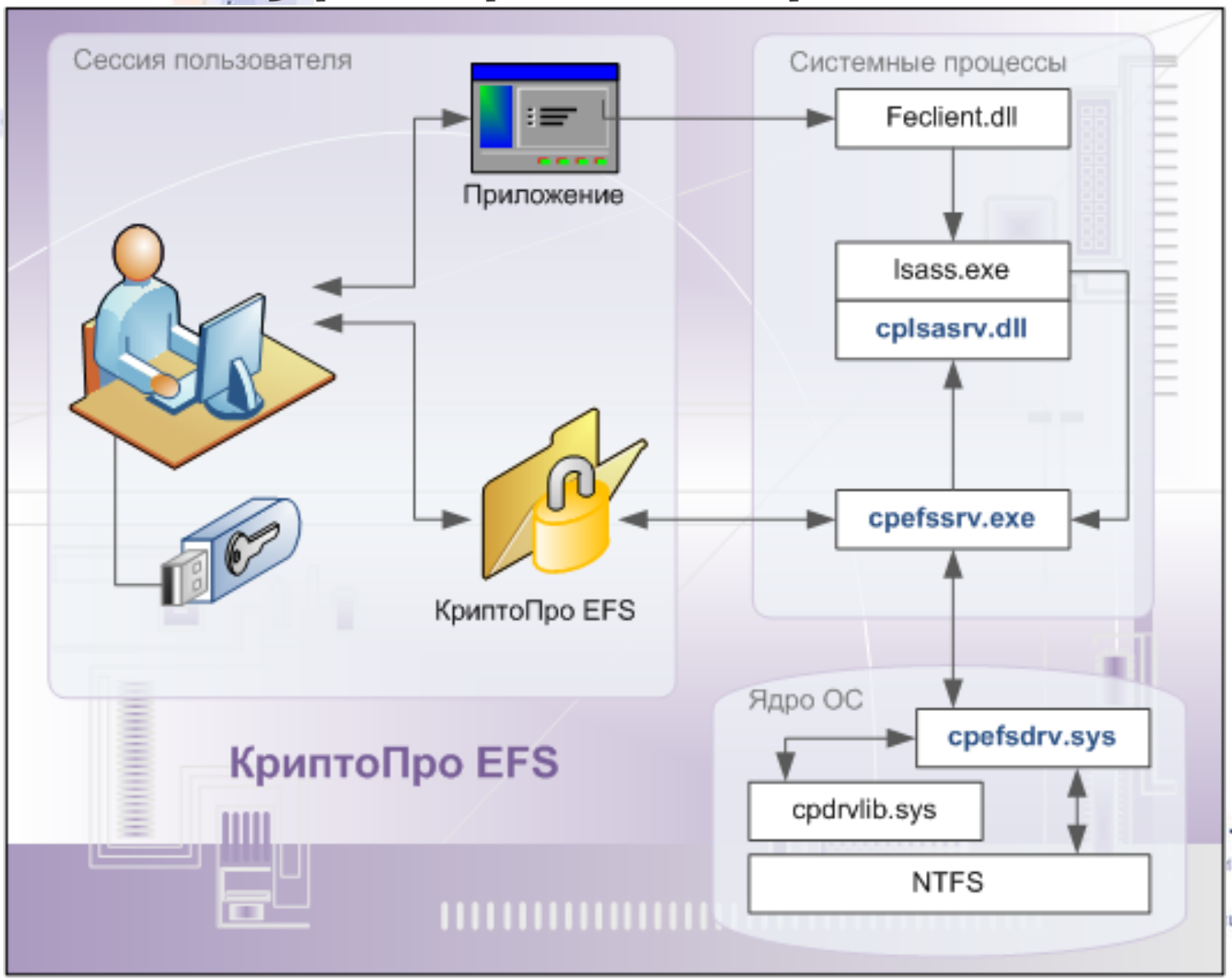
- E – Encrypting
- F – File
- S – System

Работает в файловой системе NTFS

Ключевые факты о EFS

- Шифрование файлов на уровне файловой системы
- Данные файла зашифрованы на симметричном ключе (FEK), который защищён с применением асимметричного ключа
- Возможно назначение уполномоченного агента для восстановления файлов
- Данные файла не защищены при передаче по сети

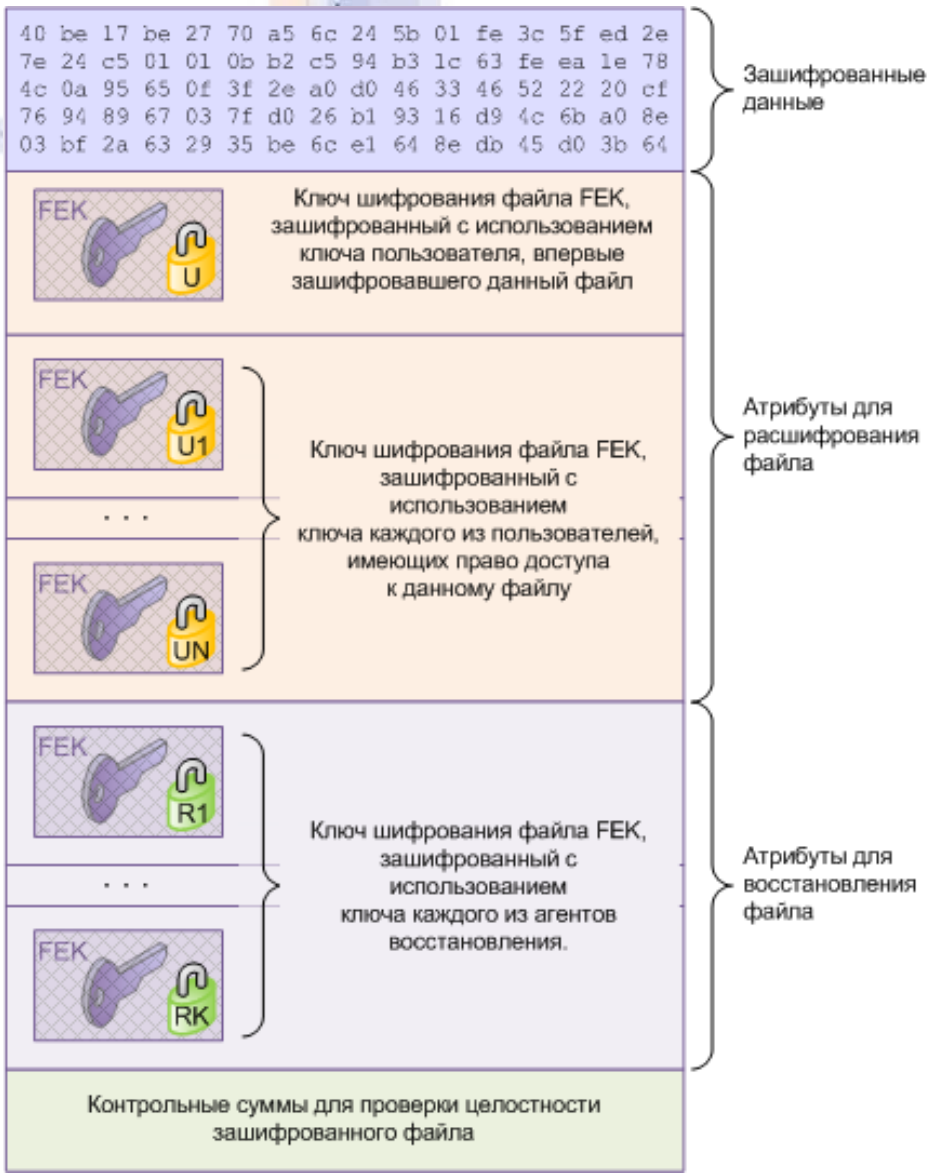
Архитектура КриптоПро и MS EFS



Дополнительные возможности КриптоПро EFS

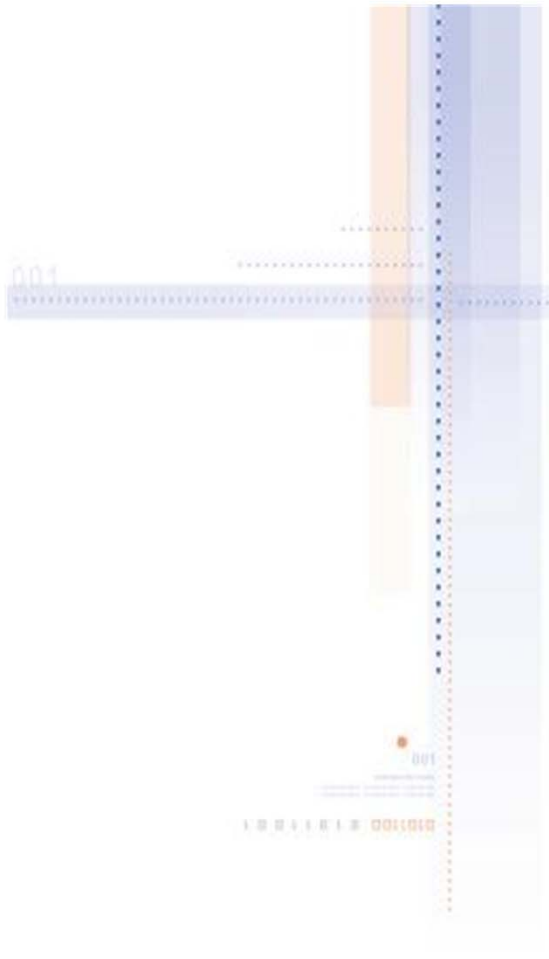
- Используются российские криптографические алгоритмы, реализованные в сертифицированном СКЗИ КриптоПро CSP
- Богатый выбор ключевых носителей
- Контроль целостности зашифрованных файлов

Формат зашифрованного файла



Пути дальнейшего развития КриптоПро EFS

- Управление ключами компьютера для удобства использования EFS в службах
- Шифрование файлов, расположенных в сети (доступ по протоколу SMB), с участием пользователя, обращающегося к ним
- Шифрование файла подкачки (pagefile.sys)



Вопросы?

Смирнов Павел
spv@cryptopro.ru