



Ключевое слово
в защите информации

Практика архивного хранения подписанных электронных документов в крупных и средних организациях

Павел Смирнов

Директор по развитию, КристоПро
Эксперт РОСЭУ

Сергей Ковтунов

Руководитель проектов, КристоПро
Эксперт РОСЭУ



ФОРУМ

РОССИЯ 20²³

- Проблема долговечности носителей
- Устаревание программного и аппаратного обеспечения
- Проблемы миграции электронных документов
- **Проблема обеспечения аутентичности, целостности, достоверности и юридической значимости документа* в течение всего срока хранения.**



* ГОСТ Р ИСО 15489-1-2019. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы

ГОСТ Р 7.0.8-2013. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения

«Архив доказательств подлинности»

- Задача: обеспечить доступность доказательств, позволяющих проверить исходные подписи документа в нужный момент времени
- Служба Архива собирает, хранит и обновляет необходимые доказательства, не создавая их самостоятельно

«Доверенный архив»

- Задача: выдать справку (квитанцию) за подписью сотрудника архива о «юридической значимости» документа в нужный момент времени
- Служба Архива доверенным образом хранит документы, полагаясь на внутренние процедуры и меры безопасности для сохранения «юридической значимости»
- Частный случай – «переподписание» документов сотрудниками архива до наступления неблагоприятных для проверяемости подписей событий

Стандарты ETSI

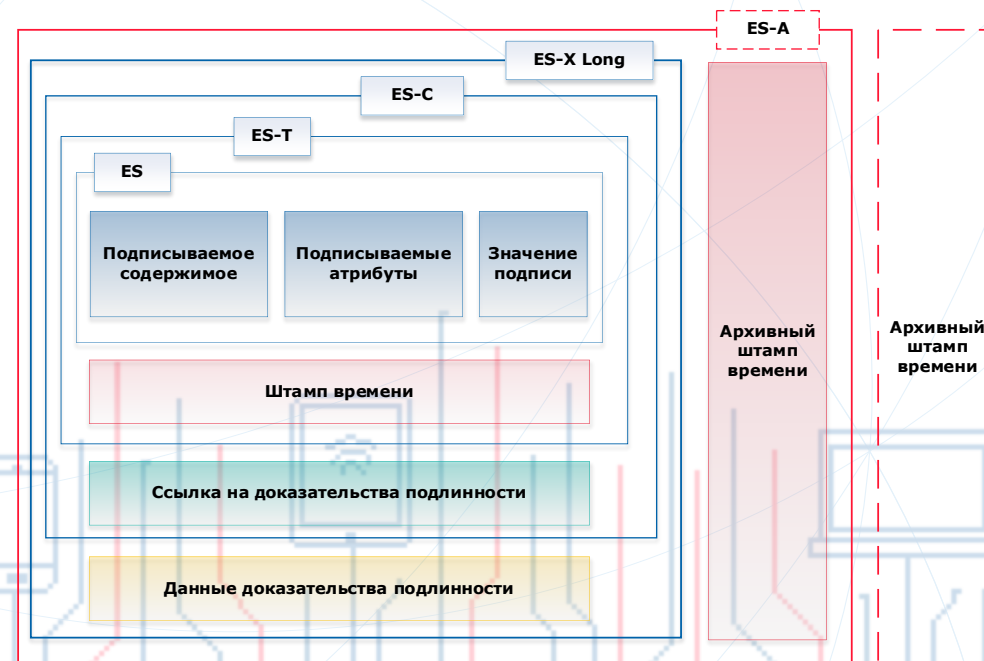
- Глубоко и широко разработанное семейство стандартов ETSI
- В ТК 26 ведётся работа по адаптации данных стандартов
- Инструменты работы с данными форматам разрабатываются с 2007 года

Стандарты AdES

- TR 119 100: Guidance on the use of standards for signatures creation and validation
- TS 119 101: Policy and security requirements for applications for signature creation and signature validation
- EN 319 102-1 & TS 119 102-1: Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
- ... (всего 42 документа)

Виды подписей AdES

- «Матрёшка» форматов от базового до архивного
- Каждый последующий вид получается добавлением доказательств к предыдущему
- Доказательствами могут быть:
 - штампы времени, OCSP-ответы, CRL, цепочки сертификатов и др.
- Цепочка архивных штампов времени позволяет продлить «срок жизни» подписи в теории бесконечно



- Дополнение электронных подписей входящего документа до формата AdES-A
- Контроль сроков действия хранящихся доказательств действительности подписей и их автоматическое обновление

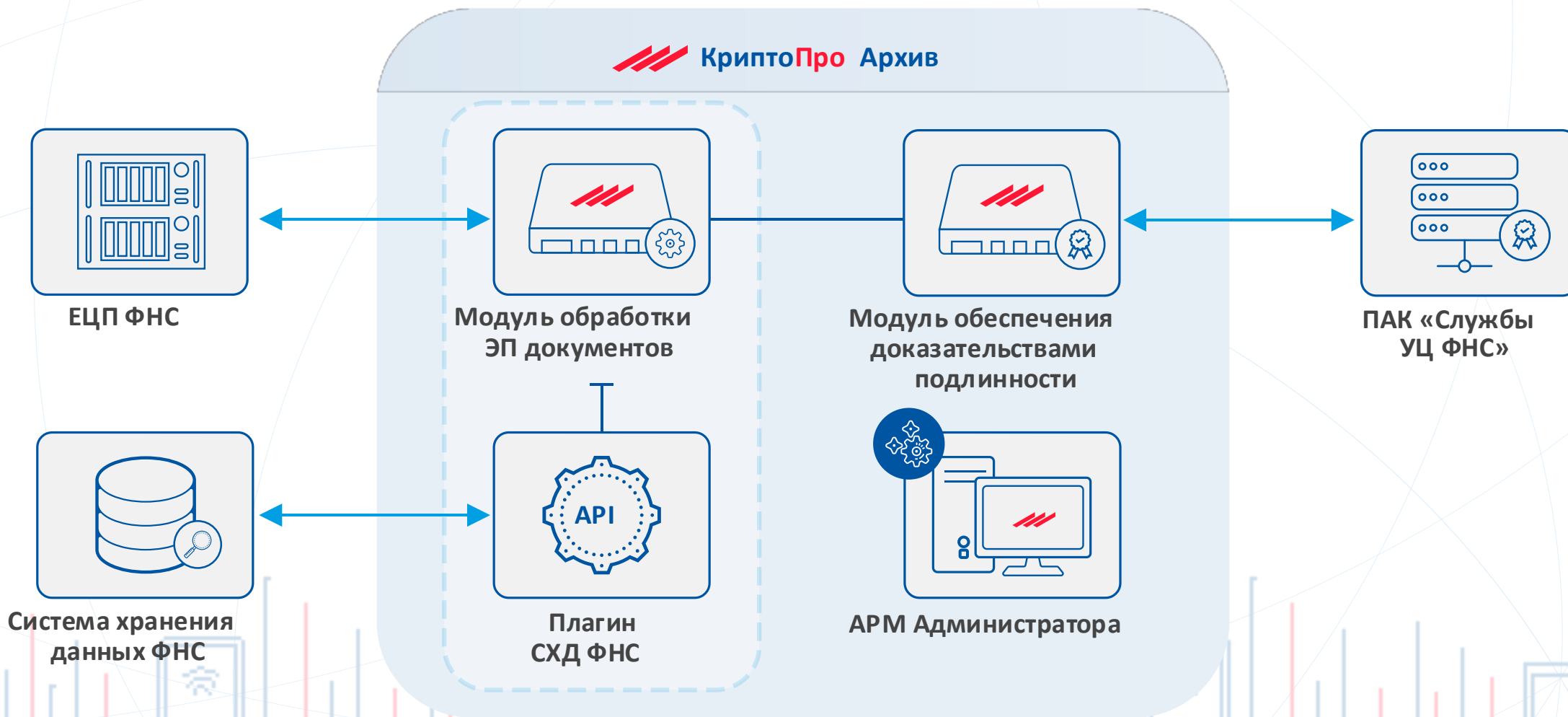


- Проверка и преобразование ЭП в формат AdES-A
- Максимальная автоматизация процессов
- Обеспечение конфиденциальности документов
- Импортозамещённые ОС и СУБД (в идеале – кроссплатформенность и поддержка разных СУБД)
- Возможность масштабирования
- Поддержка виртуализации
- Простое API для интеграции
- Поддержка интеграции с системами хранения данных (СХД)



Исходные данные

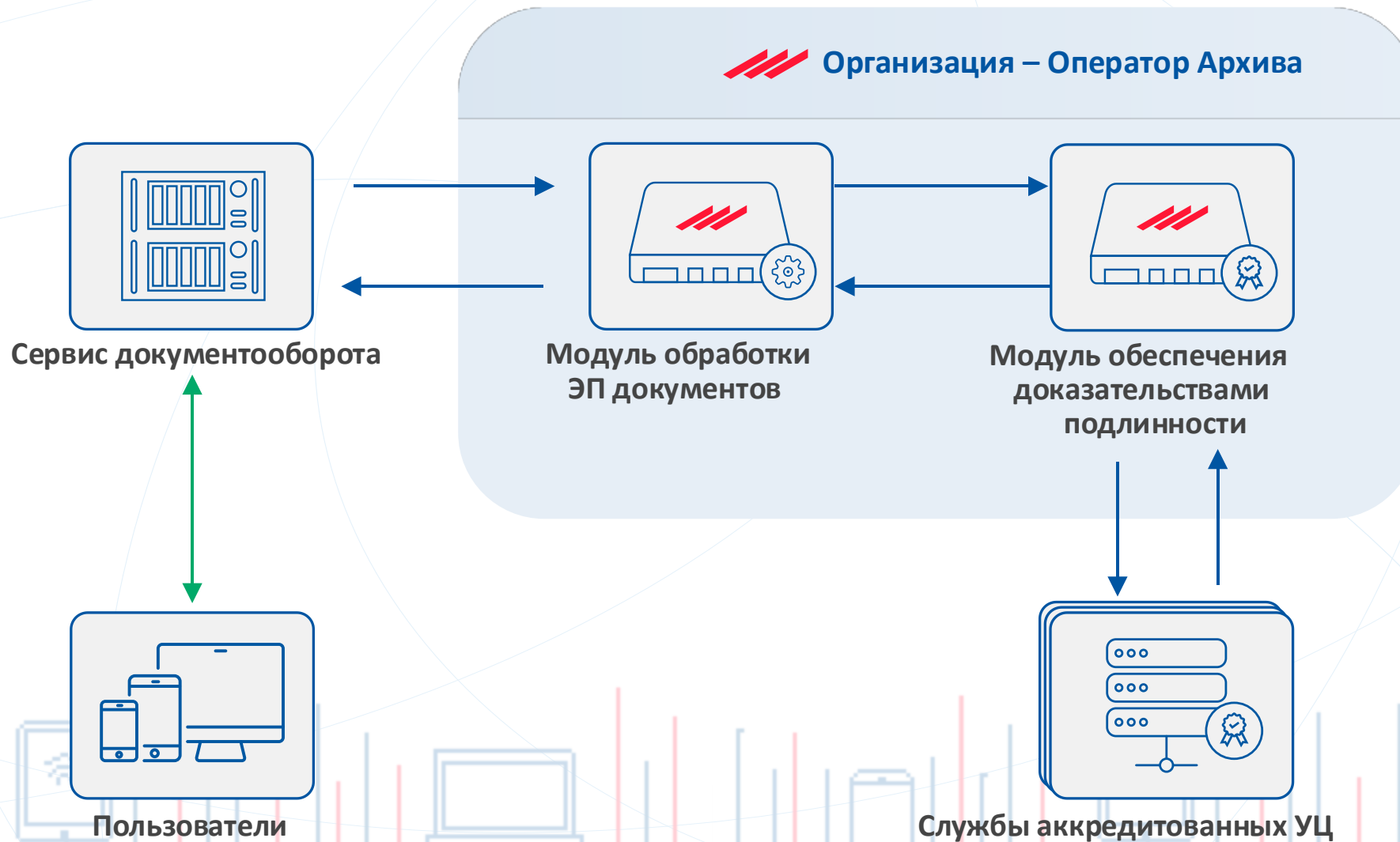
- Выпуск до 10 млн. сертификатов в год
 - Сейчас выпущено всего более 7 млн. сертификатов
- Первоначальный планируемый объем передаваемых в УЦ электронных документов в год – около 2 Тб
- Срок хранения некоторых видов документов – в течение всего срока осуществления деятельности УЦ
- Подписанные электронные документы поступают от инспекторов, заявителей, доверенных лиц



Задача	Решение
Необходимость сохранения не только подписи, но и документа	<ul style="list-style-type: none"> ■ Интеграция с СХД ФНС через разработанный плагин для КриптоПро Архив ■ Архитектурно заложена множественность плагинов
Рост количества помещаемых в архив электронных документов, и не только из УЦ	<ul style="list-style-type: none"> ■ Горизонтальное масштабирование системы ■ Максимальная автоматизация процессов
Импортозамещение	<ul style="list-style-type: none"> ■ Кроссплатформенное ПО

Предпосылки создания

- В России зарегистрировано примерно 2 млн. микро- и малых ЮЛ
- Наличие электронных документов долговременного или постоянного хранения (**но при этом их немного**)
- Ограниченный бюджет
- Система документооборота одного или нескольких операторов ЭДО
- Наличие «внутренних» электронных документов
- Необходимость создания локальных архивов документов из разных источников



Задача	Решение
Обеспечение конфиденциальности документов	<ul style="list-style-type: none"> ■ Документы не хранятся в Архиве ■ Доступ по двустороннему TLS ■ Данные разных организаций изолированы друг от друга
Рост объёма документов	<ul style="list-style-type: none"> ■ Горизонтальное масштабирование ■ Виртуализация
Интеграция сторонних СЭД с Архивом	<ul style="list-style-type: none"> ■ Простое и лаконичное API



Ключевое слово
в защите информации

СПАСИБО ЗА ВНИМАНИЕ!

127018, г. Москва, ул. Суцевский Вал, д.18

Тел./факс: +7 (495) 995-48-20

<https://cryptopro.ru>



Общие вопросы: info@cryptopro.ru
Контрактный отдел: kpo@cryptopro.ru
Для дилеров: dealer@cryptopro.ru

