КАК БАНК ВТБ РЕШИЛ УВЕЛИЧИТЬ ЮРИДИЧЕСКИ ЗНАЧИМЫЙ СРОК ЭЛЕКТРОННОЙ ПОДПИСИ И ЧТО ИЗ ЭТОГО ПОЛУЧИЛОСЬ?

Спикер:
Алена Голубцова
Ольга Ващенкова

20 марта
2025 год

Алёна Голубцова

Директор по управлению проектами

Стрим «Обработка и архив документов», ПАО ВТБ

ASGolubcova@vtb.ru

Alena_Glbs

+7(916) 246-83-34

Ольга Ващенкова

Руководитель службы проекта реализации УЦ

ООО «ГК ИННОТЕХ»

Ovaschenkova@inno.tech

@green5tree

+7(903) 577-51-17

Почему ПАО ВТБ решил начать проект по внедрению долговременного хранения электронных документов

>90%

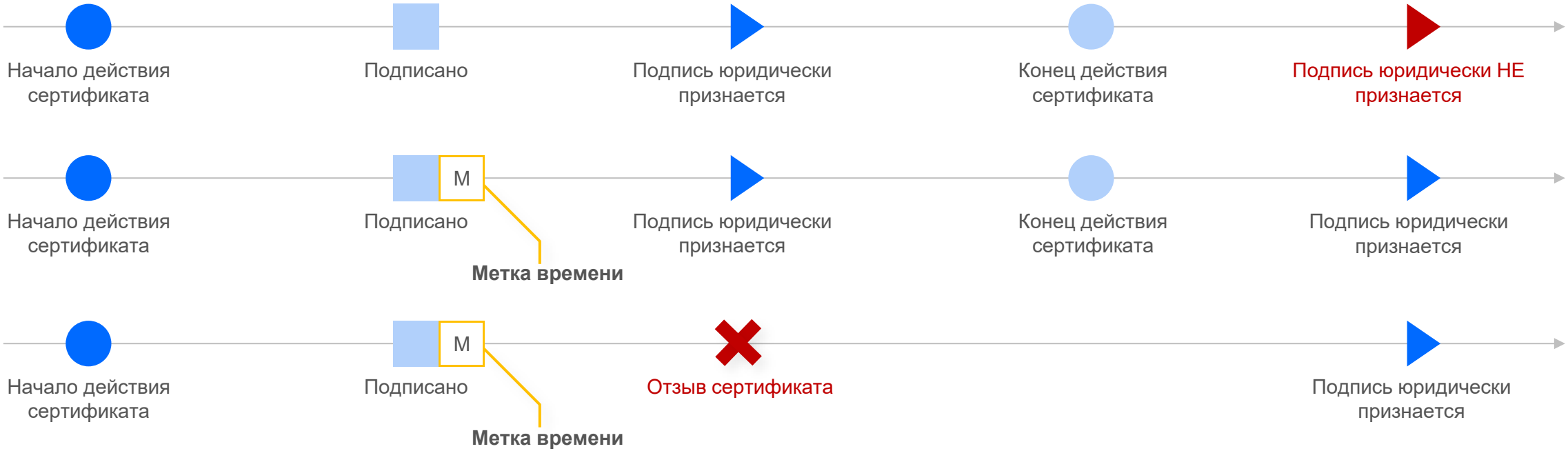
Всего документооборота в 2020-2022 г переведено в цифровой формат в результате программы «Безбумажный банк»

>1 МЛН

Документов ежедневно сохраняется в структурированном электронном архиве банка «ИНТАР»

Растет потребность в обеспечении долговременного неизменного хранения ЭП

Проблема хранения документа, подписанного ЭП



Метка Доверенного Времени (МДВ) — доказательство существования подписанного документа в указанный момент времени

Ответ OCSP службы – это значение статуса сертификата ЭП в указанный момент времени

Как добавить Метку Доверенного Времени (МДВ) к электронным подписям, поступающим в банк?

Как обеспечить долговременное хранение подписи в электронном архиве Банка при постоянном обновлении стандартов криптографии?

Как максимально продлить срок юридической значимости предоставленной ЭП ?

Предложенное решение

01.

Модернизировать УЦ ВТБ, развернуть собственную TSP(1) и OCSP(2) службы

02.

Научиться обогащать все подписи метками доверенного времени (МДВ)

03.

Усиливать подписи с МДВ до формата архивного хранения CADES-A, который увеличивает срок получения положительного результата проверки подписи

(1) — TSP – Time Stamp Protocol – криптографический протокол, позволяющий создавать доказательство факта существования электронного документа на определенный момент времени.
(2) — OCSP – протокол, используемый для получения статуса цифровых сертификатов ЭП.

Наш план действий

1. Анализ рынка, оценка разработки собственными силами

2. Заключение договора с КриптоПро на поставку линейки продуктов под тех стек Astra Linux

3. Внедрение:

- Криптосервера
- Удостоверяющего центра, включая службы TSP и OCSP
- Архива в ландшафт Банка, интеграция со смежными системами, переключение всех потребителей

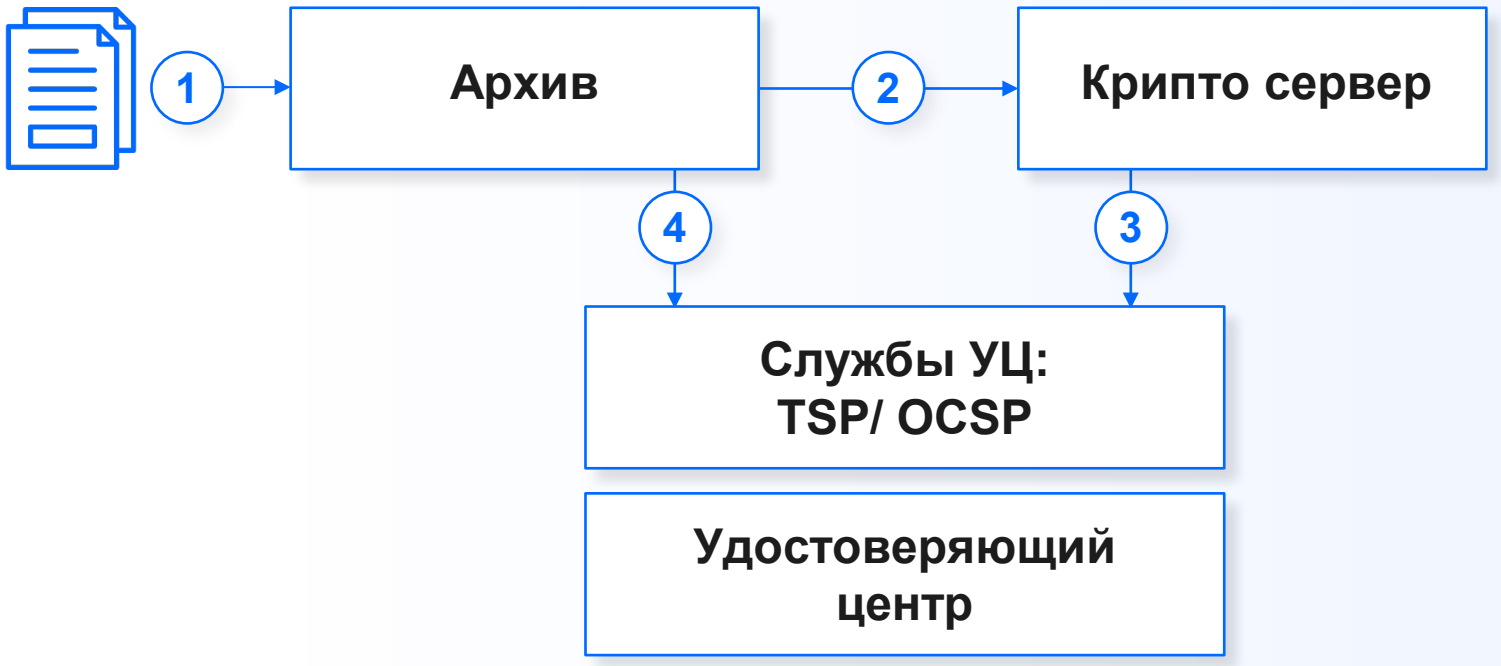
4. Расширение функциональных возможностей:

- Усиление CADES-BES подписей до CADES-T и CADES-XLT1
- Усиление CADES-XLT1 до CADES – A

5. Анализ полученных результатов, формирование бэклога развития

Как подпись становится архивной?

CADES-BES (Basic Electronic Signature) > **CADES-XLT1** (Extented) > **CADES-A** (Archival)



1. Загрузка в архив документа и подписи в формате CADES-BES
2. Запрос на усиление подписи
3. Обращение к службам УЦ для усиления подписи до CADES-XLT1
4. Обращение к службам УЦ для усиления подписи до CADES-A

СЮРПРИЗЫ И …

Даже при наличии собственной TSP службы не можем проставить МДВ (1) на сертификаты подписей, выпущенных сторонними УЦ

… И ВОПРОСЫ

44 аккредитованных внешних АУЦ. Как получать доказательство действительности сертификатов ЭП от каждого из них?

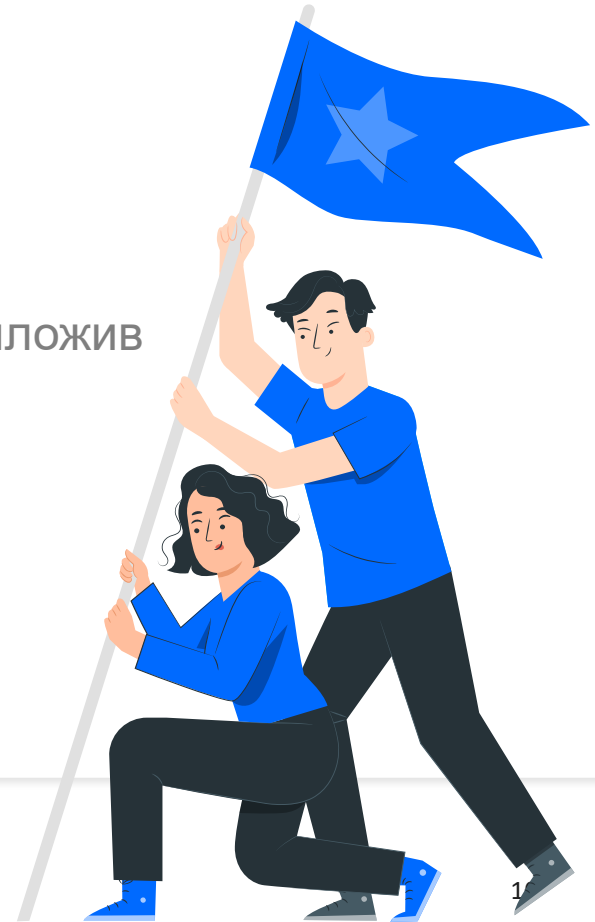
Как подтверждать действительность сертификатов ЭП, выпущенных УЦ, у которых нет своей OCSP(2) службы?

(1) — МДВ – метка доверенного времени
(2) — OCSP – протокол, используемый для получения статуса цифровых сертификатов ЭП

Обсудили с экспертами из КриптоПро и МинЦифры возможные подходы

РЕЗУЛЬТАТЫ ОБСУЖДЕНИЯ:

- Подтвердить действительность сертификата подписи в момент проверки может только УЦ, который выпустил сертификат подписи
- Получить подтверждение действительности можно либо через протокол OCSP(1) при наличии соответствующей службы в УЦ, либо приложив CRL(2)
- Необходима настройка интеграции со службами OCSP всех 44 аккредитованных УЦ



(1) — OCSP – протокол, используемый для получения статуса цифровых сертификатов ЭП
(2) — CRL – Certificate Revocation List – Список отозванных сертификатов

Влияние результатов обсуждения на проект

Увеличение объема задач проекта для расширения интеграции с OCSP службами УЦ

Увеличение объема задач проекта для реализации сохранения CRL для сертификатов тех УЦ, у которых нет OCSP службы

Увеличение ожидаемого объема хранимых файлов подписей в формате CADES-A (с 50 КБ до 5 МБ) для некоторых УЦ при добавлении CRL

- увеличение объема инфраструктурных мощностей для сохранения быстродействия и возможности хранения
- увеличение изначально заложенного бюджета на мощности

Но это еще не все….

Нас ждал сюрприз:
Два аналогичных шага в процессе настройки цепочки доверия

ИЗНАЧАЛЬНО КОНСТРУИРУЕМЫЙ ПРОЦЕСС

Архив передает файл подписи на обогащение

КриптоПро Ключ Light связывается с УЦ и обогащает до формата XLT1. Возвращает обратно в Архив

Настройка корневых сертификатов для всех 44 УЦ

Архив передает файл в формате XLT1 в КриптоПро Архив

КриптоПро Архив идет в УЦ ВТБ, получает вторую МДВ, перештамповывает в CADES-A и передает обратно в Архив на хранение

КАК ПРОЦЕСС ЗАРАБОТАЛ НА САМОМ ДЕЛЕ

Архив передает файл подписи на обогащение

КриптоПро Ключ Light связывается с УЦ и обогащает до формата XLT1. Возвращает обратно в Архив

Настройка корневых сертификатов для всех 44 УЦ

Архив передает файл в формате XLT-1 в КриптоПро Архив

КриптоПро Архив идет в УЦ ВТБ, получает вторую МДВ, перештамповывает в CADES-A и передает обратно в Архив на хранение

Настройка корневых сертификатов для всех 44 УЦ

60 МИНУТ

Настройка 1 УЦ в 1 решении

43 УЦ

Требуется настроить

МЕСЯЦ В ЧЕЛОВЕКО-ДНЯХ

Только на настройку цепочки доверия

#1.

Заранее создать список УЦ, подписи которых вы хотите обогащать до архивного формата и обеспечить получение их корневых сертификатов

#2.

Не забыть про инструменты для сбора статистики (УЦ, форматы подписей, размеры файлов подписей после обогащения и т.п.)

#3.

Запланировать достаточное количество инфраструктурных мощностей для хранения довольно тяжелых подписей, обогащенных CRL, выпущенных теми УЦ, у которых нет OCSP служб

#4.

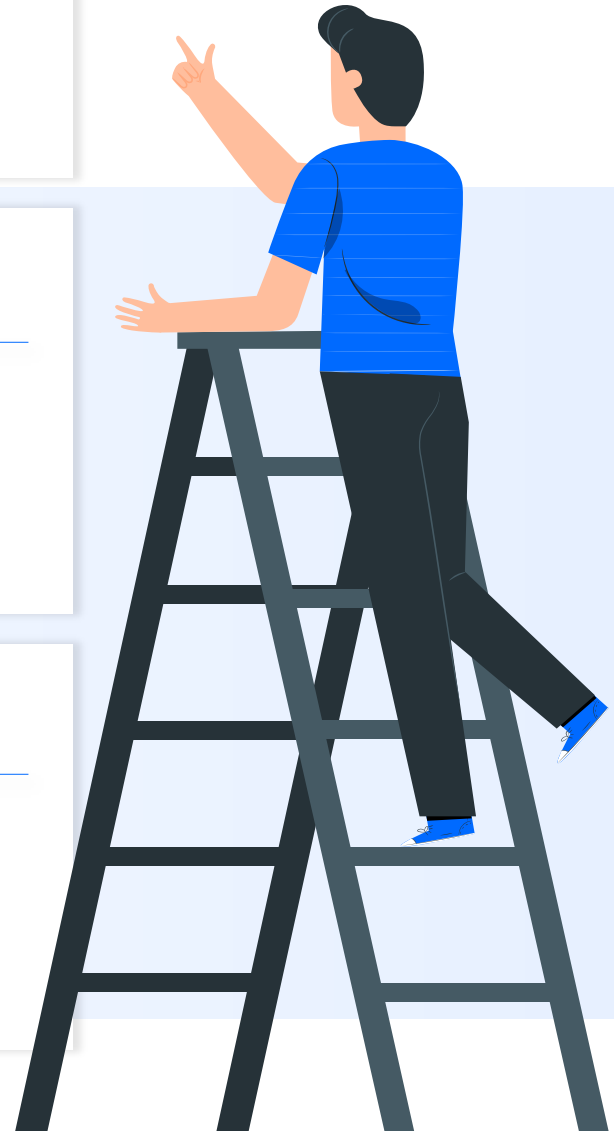
Учесть дополнительные ресурсы для поддержки процесса настроек корневых сертификатов для выбранных УЦ на протяжении всей выстраиваемой цепочки доверия

#5.

Внести в план работы по интеграции с OCSP службами УЦ для всех продуктов КриптоПро, участвующих в цепочке доверия, выстраиваемой в вашей организации

#6.

Продумать процессы мониторинга сроков действия корневых сертификатов в цепочке доверия и их автоматического обновления для бесперебойной работы всего процесса



#1. Идеи для регулятора

Было бы здорово, если бы существовал единый агрегированный сервис, подтверждающий действительность сертификатов, выпущенных любыми удостоверяющими сервисами с единой OCSP службой

Или было бы здорово законодательно обязать все АУЦ иметь общедоступные OCSP службы

#2. Идеи для продактов из компании КриптоПро

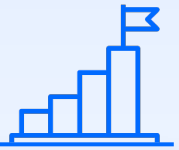
Нам, как пользователям вашего продукта, не хватает единого решения для обновления корневых сертификатов и оркестрации ими, которое бы раздавало настройки цепочек доверия автоматом сразу всем установленным в организации продуктам КриптоПро.

Первые результаты

#1

За первые 2 недели работы сервиса обогащено более 2 000 подписей

#2



Стали мега-популярным продуктом в банке, так как все хотят обогащать подписи до формата архивного хранения и хранить свои документы у нас

#3

Расширяем сервисную модель за счет присоединения новых бизнес-доменов

#4

Готовимся выйти на рынок решений архивного хранения электронных документов с продуктом «ИНТАР», где будем предлагать функционал обогащения подписей МДВ и усиления их до архивного формата хранения

СПАСИБО ЗА ВНИМАНИЕ!

Алёна Голубцова

Директор по управлению проектами

Стрим «Обработка и архив документов», ПАО ВТБ

ASGolubcova@vtb.ru

Alena_Glbs

+7(916) 246-83-34

Ольга Ващенкова

Руководитель службы проекта реализации УЦ

ООО «ГК ИННОТЕХ»

Ovaschenkova@inno.tech

@green5tree

+7(903) 577-51-17