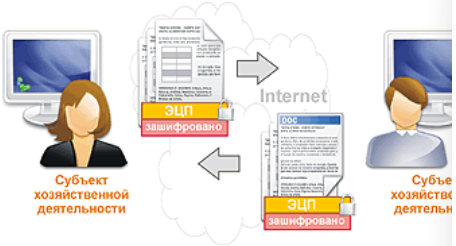
infotecs

XII международная конференция
«PKI-Forum Россия 2014»

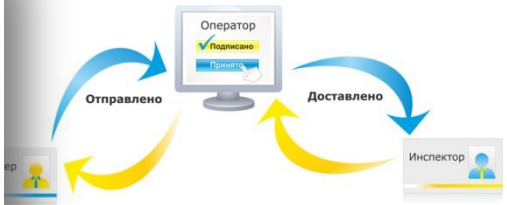
# Как проверить подпись через 100 лет? Взгляд ИнфоТеКС

Кийко Александр
менеджер проектов
KykoAS@infotecs.ru

Система межведомственного электронного взаимодействия


Обмен документами между
Субъектами хозяйственной деятельности


Сдача отчетности в
контролирующие органы

Единый портал государственных услуг

Как будет обеспечена юридическая значимость документов через длительный интервал времени?

Как будет обеспечена возможность проверки валидности ЭП, которая была поставлена несколько лет назад?

Как доказать, что подпись, поставленная несколько лет назад, соответствовала валидному сертификату ЭП?

Метод «снятия ЭП»: при приеме документа на архивное хранение подписи проверяются, результаты проверки документируются, все содержащиеся в ЭП сведения заносятся в метаданные документа.

Метод «архивных ЭП» оставляет ЭП под документом, но при этом для продления срока действия ЭП осуществляется дополнение ЭП рядом параметров, т.е. осуществляется переход к усовершенствованной ЭП

# Что же дает нам реализация стандарта CAdES?

## Защита от некоторых атак

Атака, связанная с подменой сертификата подписанта

Отсутствует информация, что в момент создания подписи подписант имел право создавать данную подпись

Отсутствует доверенное время создания подписи

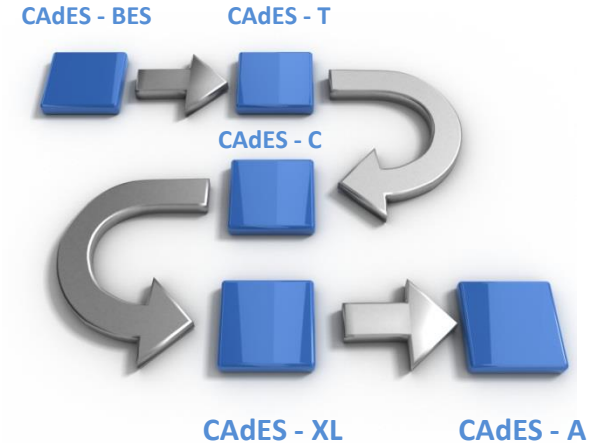
## Возможность офлайн проверки подписи

## Увеличение срока действия подписи

- Уберечься от компрометации использованный при создании подписи криптографических ключей;
- Уберечься от достижения предельного срока эксплуатации для использованных при создании подписи сертификатов;
- Уберечься от изменения в будущем структуры цепочек удостоверяющих центров;
- Для подписи формата CMS нет возможности уберечься от изъятия доказательств подлинности отдельных сертификатов

# Стандарт CAdES

Формат CAdES включает несколько форм представления усовершенствованной подписи. Зачастую эти формы накладываются друг на друга, образуя некую слойную структуру, накладываясь одна на другую.



## CAdES - BES

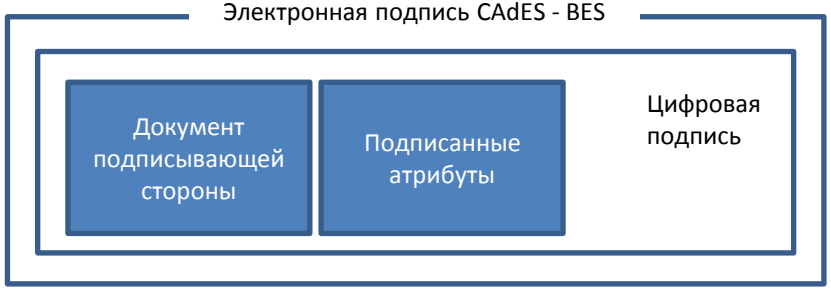
Формируется на клиентском месте, где осуществляется подписание документа

CAdES - T

CAdES - C

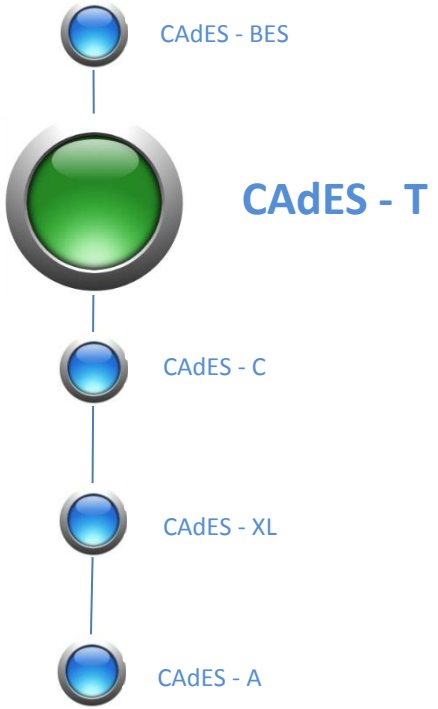
CAdES - XL

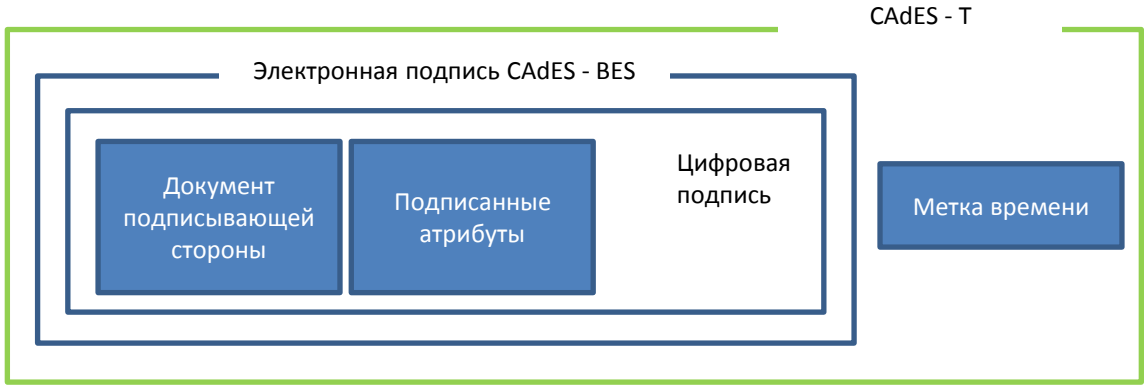
CAdES - A




Что делается? Добавляется хэш сертификата + OID алгоритма хэш-функции

Что это нам дает? Защита от подмены сертификата



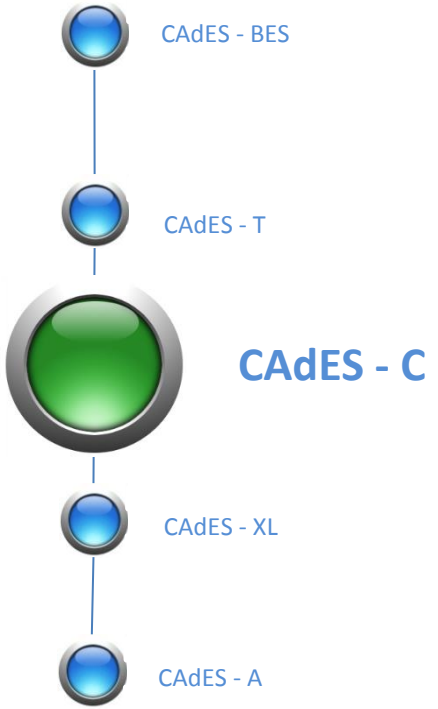



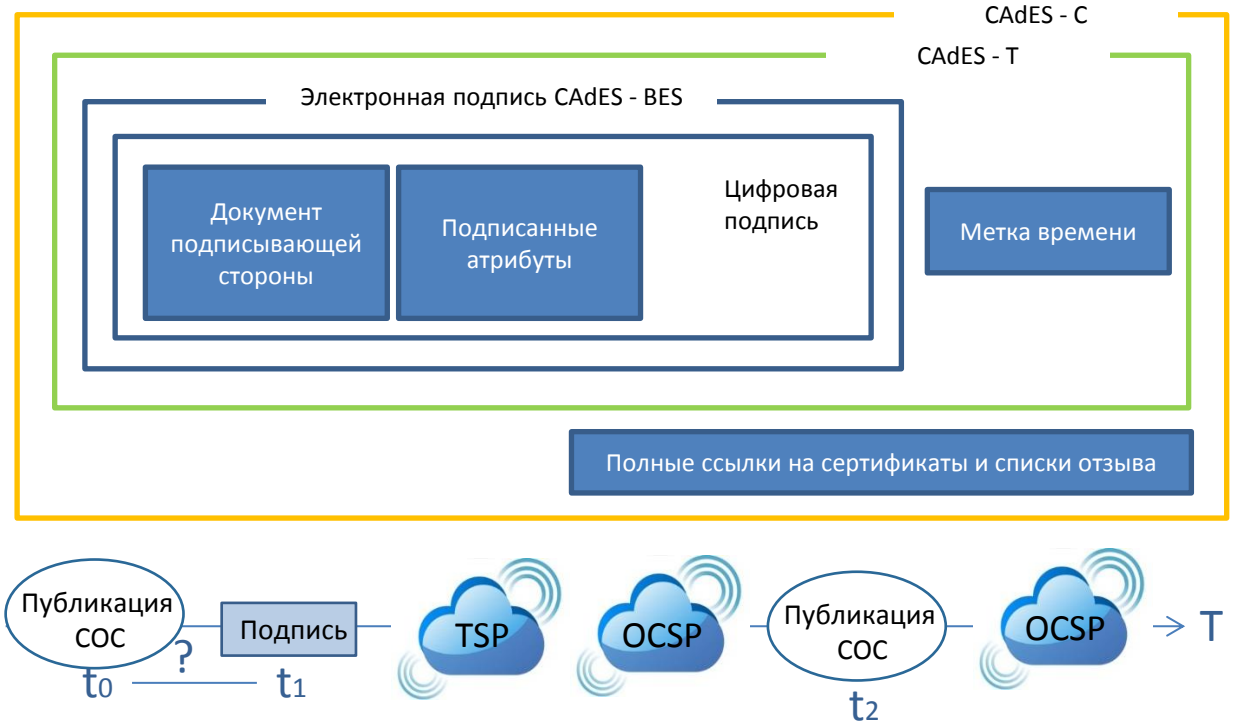

## Что делается? Добавляется штамп времени

## Что это нам дает?

Доказательство времени создание подписи не позднее времени, указанном в штампе.

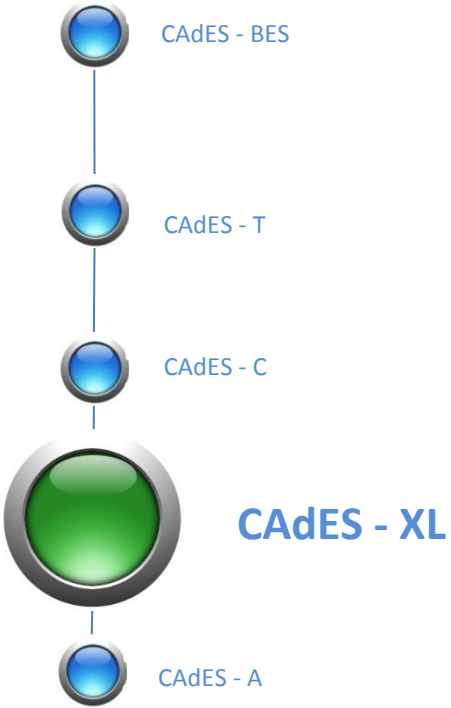
Штамп времени будет использоваться для доказательства того, что сертификат подписанта не был отозван в момент создания подписи

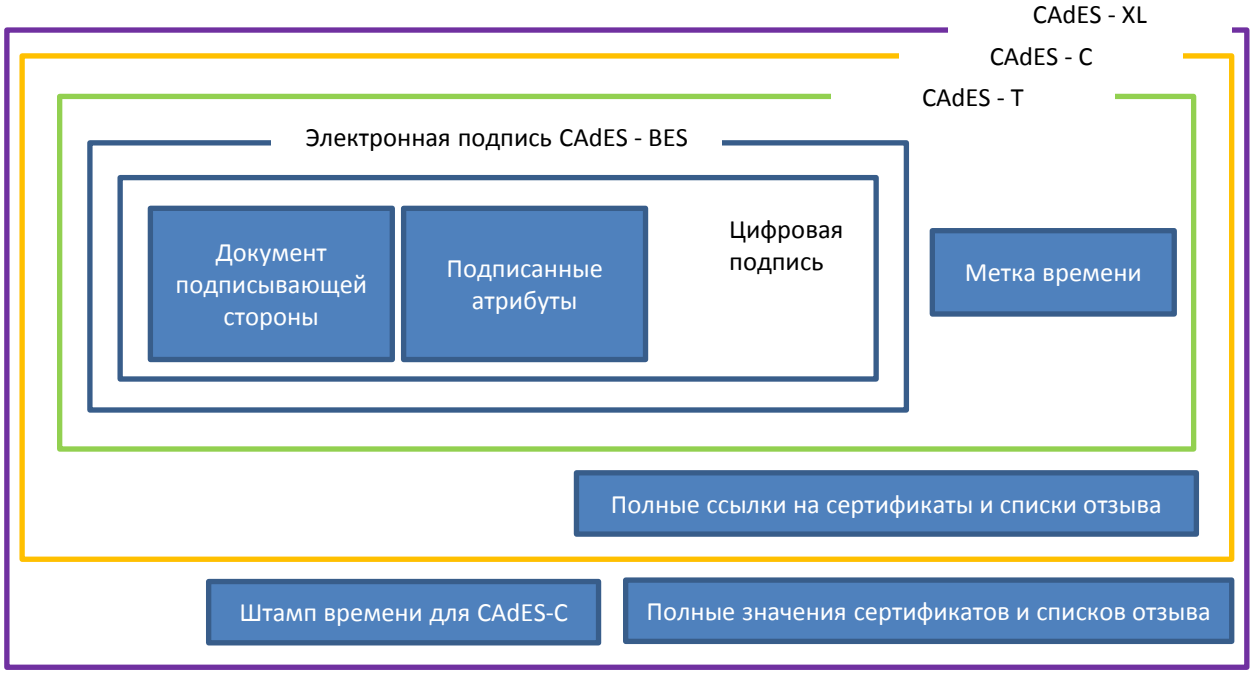



## Что это нам дает?

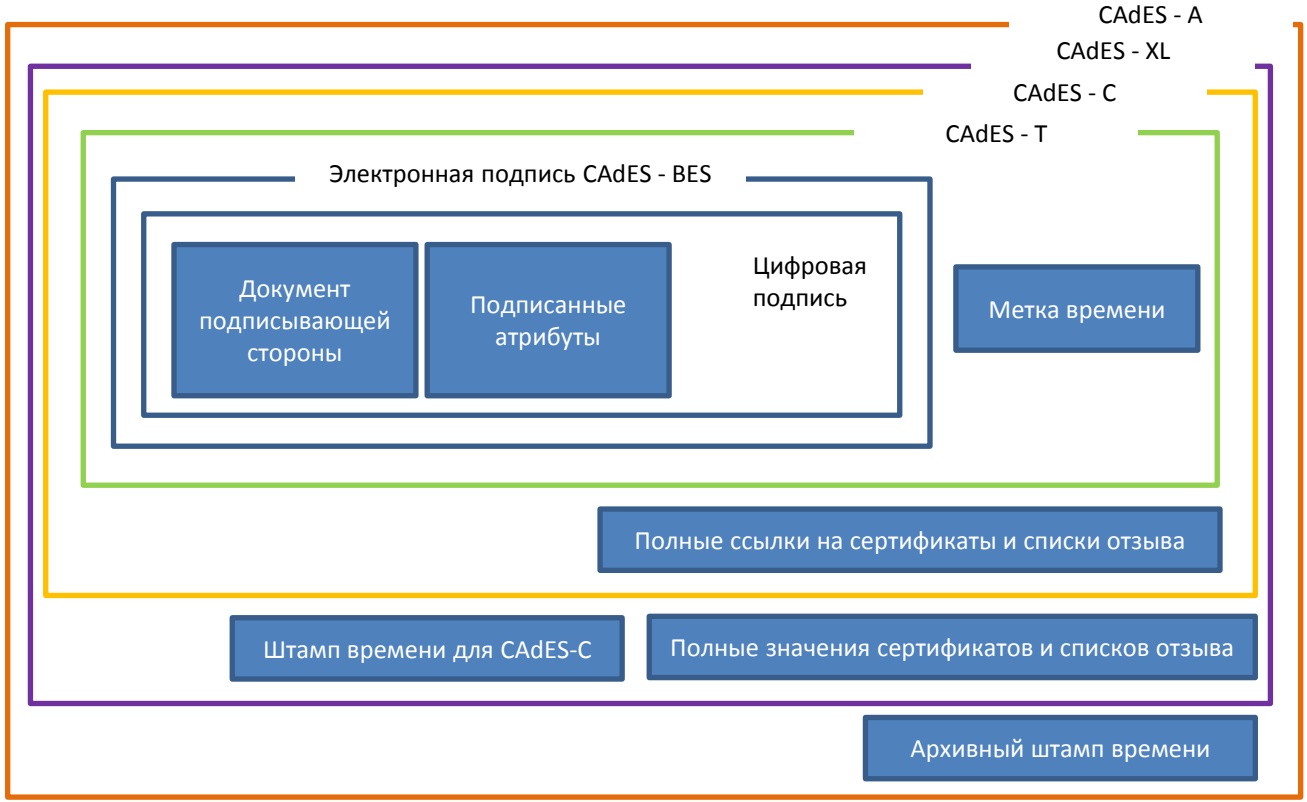
Гарантия, что сертификат не был отозван в момент подписи




## Что это нам дает?

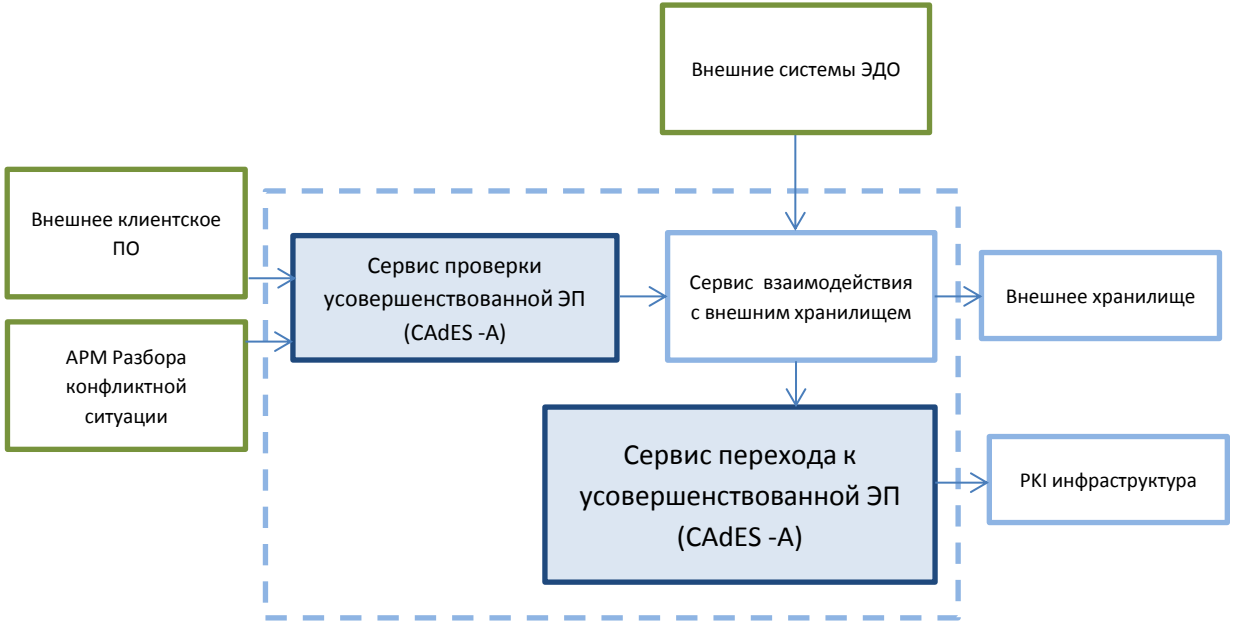
Возможность офлайн проверки подписи


**CAdES - A**

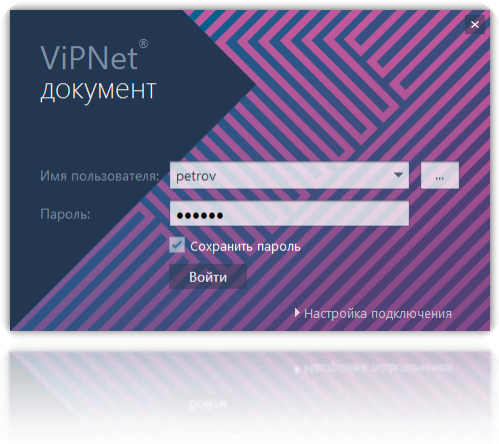
Что это нам дает? Увеличение срока действия подписи

# Укрупненная схема решения по работе с усовершенствованной ЭП



# Решение интегрировано с системой ViPNet ЭДО Документ и находится на стадии опытной эксплуатации

ViPNet ЭДО Документ




Сервер оператора ЭДО

Сервер усовершенствованной ЭП

# Спасибо за внимание!
# Вопросы?

Кийко Александр
менеджер проектов
KykoAS@infotecs.ru