11 СЕНТЯБРЯ 2025

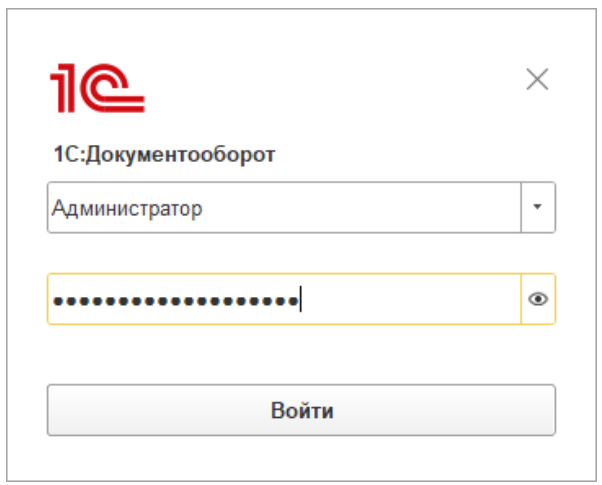
2-я конференция «Практика 1С:ЭДО»

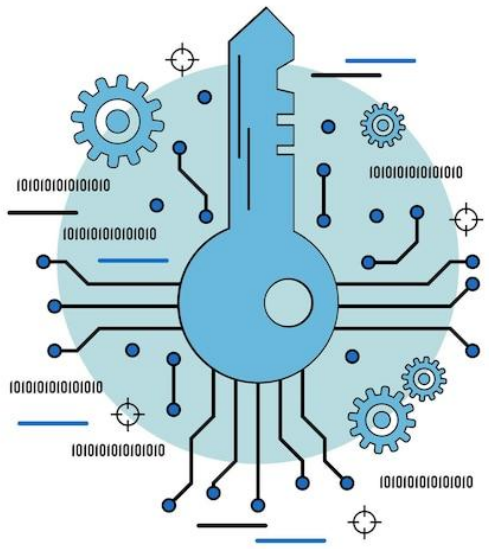
Что важно знать про электронные подписи разных форматов

Александр Федай,
Руководитель разработки 1С:Архива, «1С»

Виды электронных подписей

- **По способу формирования и уровню защиты:**
  - **Простая – основана на использовании паролей и кодов для подтверждения подписания**
  - **Усиленная – формируется с использованием криптографического преобразования информации, позволяет обнаружить факт внесения изменений в данные после подписания**





Виды усиленных электронных подписей

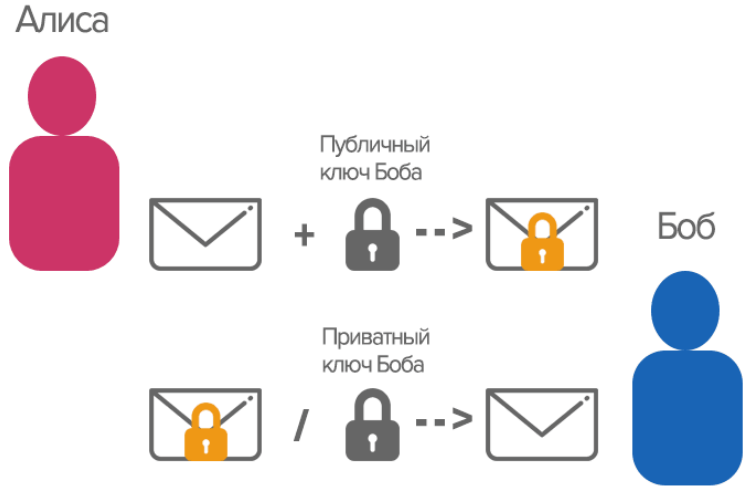
- **По статусу удостоверяющего центра, выдавшего сертификат:**
  - **Квалифицированная (УКЭП) – выдана аккредитованным УЦ, использующим сертифицированные ФСБ средства**
  - **Неквалифицированная (УНЭП) – может быть выдана любым УЦ, в т.ч. собственным УЦ предприятия**

Виды усиленных электронных подписей

- По отношению к подписываемым данным:
  - Отсоединенная
  - Присоединенная

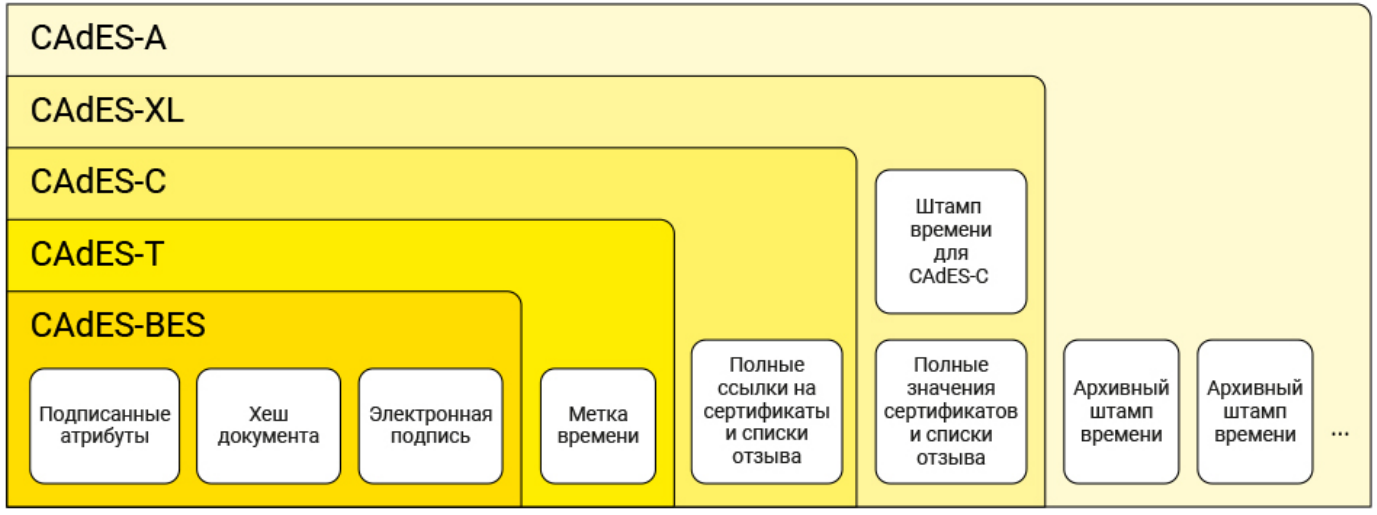
Виды усиленных электронных подписей

- По виду используемого алгоритма:
  - ГОСТ
  - RSA
  - …



Виды усиленных электронных подписей

- По составу включаемых в подпись данных
  - Стандарт CAdES (CMS Advanced Electronic Signatures)
  - Каждый следующий формат содержит данные предыдущего + дополнительные данные
  - Один формат можно преобразовать в другой, подпись при этом не «испортится»

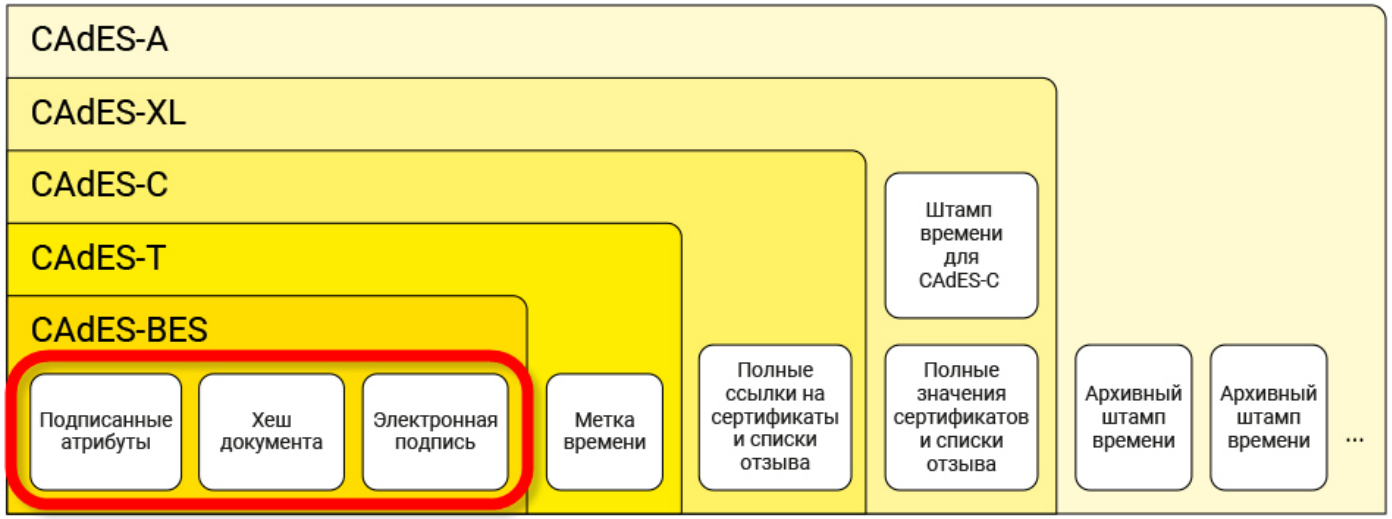


Данные для проверки ЭП

- При проверке ЭП необходимо подтвердить, что
  - Был подписан именно этот файл, а не какой-то другой
  - Сертификат выдан доверенным УЦ
  - Сертификат не истек на момент подписания
  - Сертификат не был отозван на момент подписания
    - Или на момент проверки, если момент подписания не определен

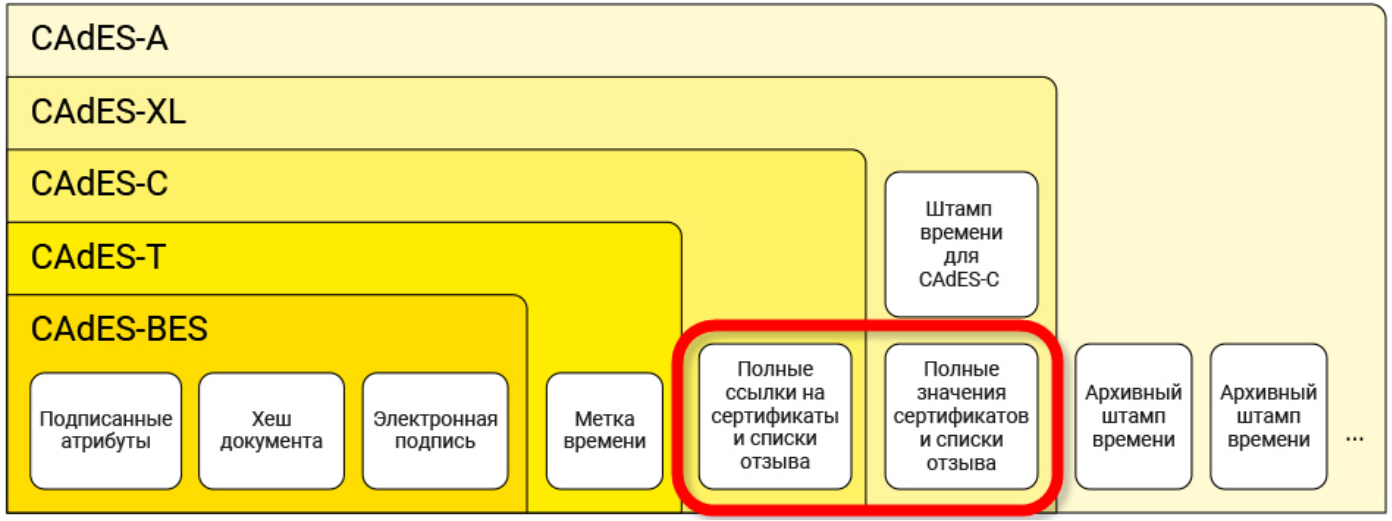
Данные для проверки ЭП

- **Был подписан именно этот файл**
  - **Базовые данные: хеш-сумма файла, алгоритм ЭП, результат преобразования хеш-суммы с использованием алгоритма и закрытого ключа сертификата, данные о подписывающем лице**
  - **В наличии всегда**



Данные для проверки ЭП

- Сертификат выдан доверенным УЦ, Сертификат не был отозван
  - Сведения о цепочке сертификатов – ссылки (идентификаторы) или полные значения
  - Список отзыва сертификатов – ссылки или полные значения
- Если сведения о сертификатах отсутствуют (CAdES-BES), при проверке они загружаются с ресурса УЦ



Данные для проверки ЭП

- Сертификат не истек на **момент подписания**
- Сертификат не был отозван на **момент подписания**
  - Или на момент проверки, если момент подписания не определен

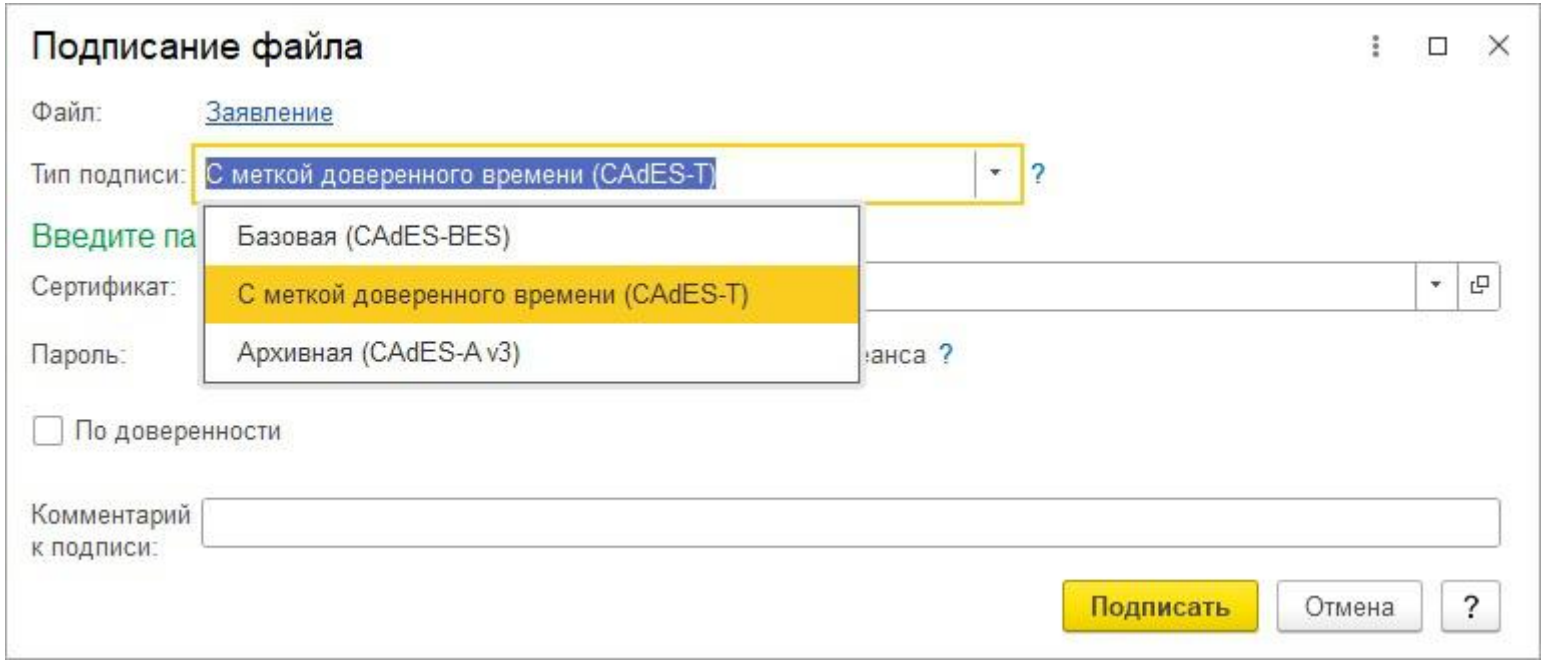
Данные для проверки ЭП

- Метка времени (штамп времени, TSP-ответ)
  - 63-ФЗ: «метка доверенного времени – это достоверная информация в электронной форме о дате и времени подписания электронного документа»
  - Технически это подпись, где в качестве подписанных данных выступают хеш базовой подписи и текущее точное время
  - Метку времени предоставляет специальная TSP-служба (Time Stamp Protocol)
  - Сертификат метки тоже имеет свой срок, но он, как правило, более длительный (до 15 лет)

Данные для проверки ЭП

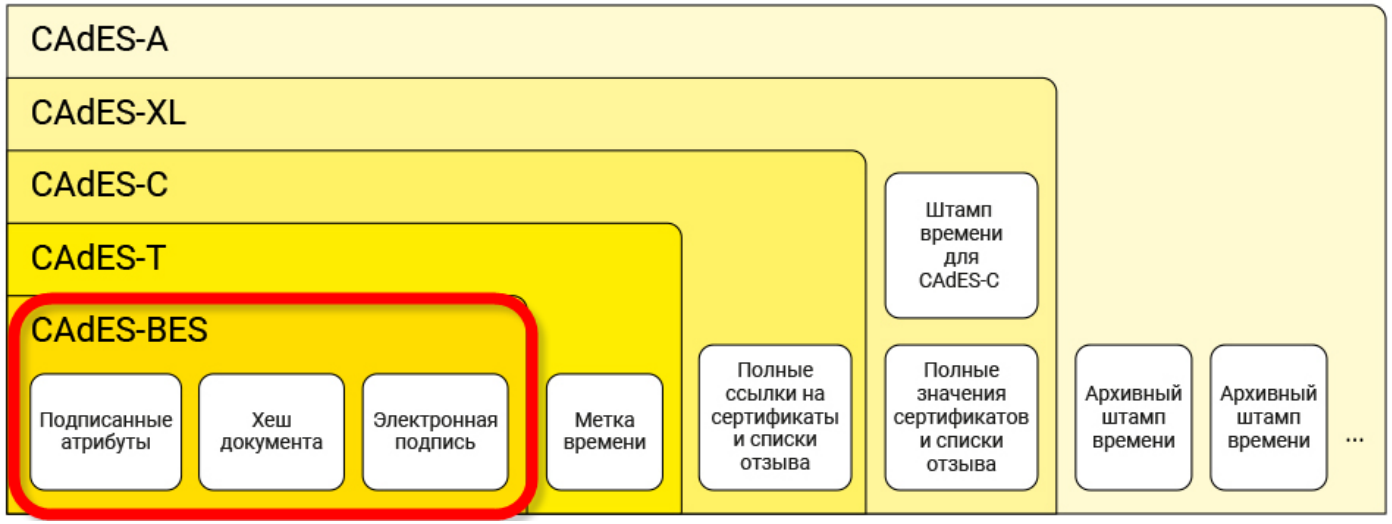
- Сертификат не истек на **момент подписания**
- Сертификат не был отозван на **момент подписания**
  - Или на момент проверки, если момент подписания не определен

Форматы ЭП при подписании в 1С



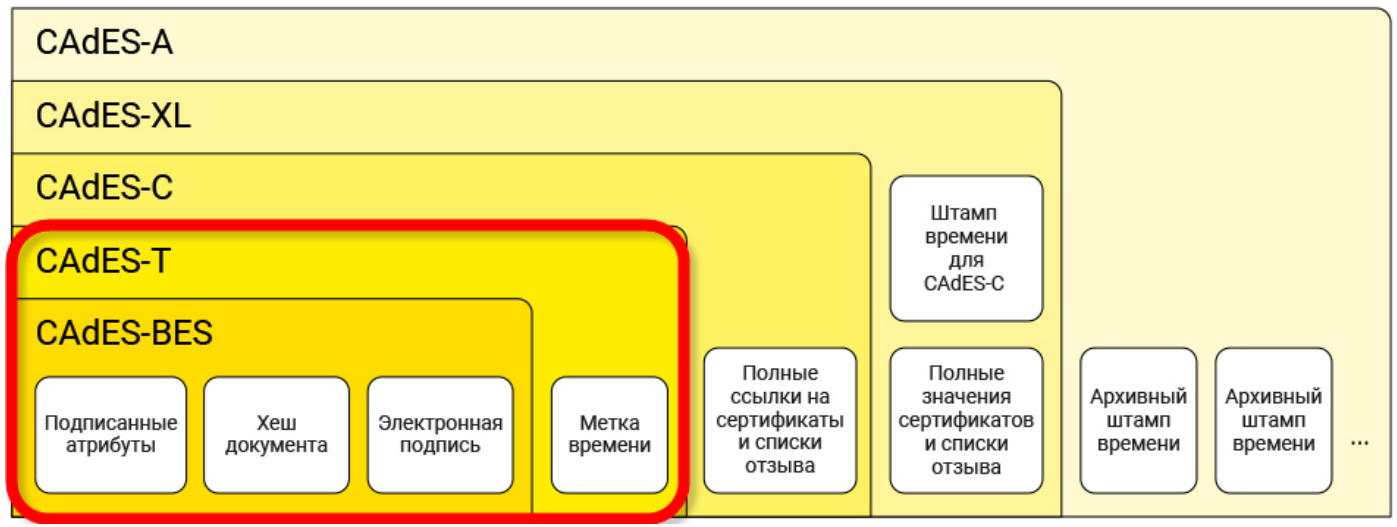
Формат CAdES-BES (базовая ЭП)

- **Базовые данные**



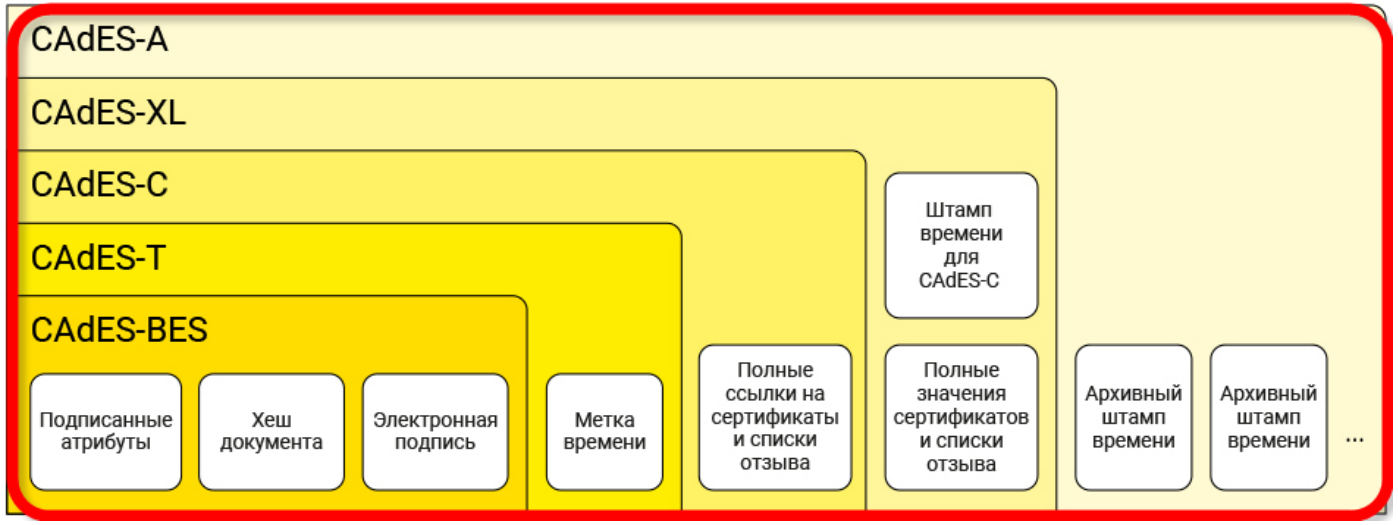
Формат CAdES-T (с меткой времени)

- **Базовые данные**
- **Метка времени для подтверждения момента подписания**



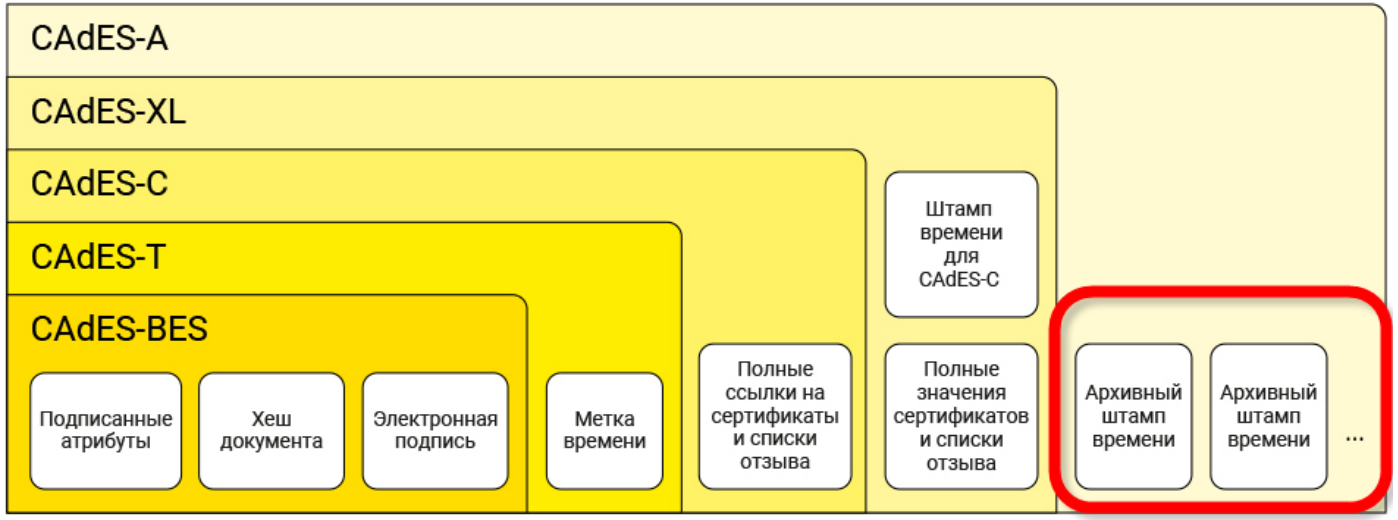
Формат CAdES-A (архивная)

- **Базовые данные**
- **Метки времени**
- **Полные данные о сертификатах и списках отзыва**



Формат CAdES-A (архивная)

- Предполагает добавление новых архивных меток в процессе хранения ЭП
- Если срок действия предыдущей метки подходит к концу, можно добавить новую метку, продлевая достоверность всех данных на срок сертификата новой метки
- Защита от устаревания алгоритмов подписи: новые штампы могут использовать новые, более современные алгоритмы

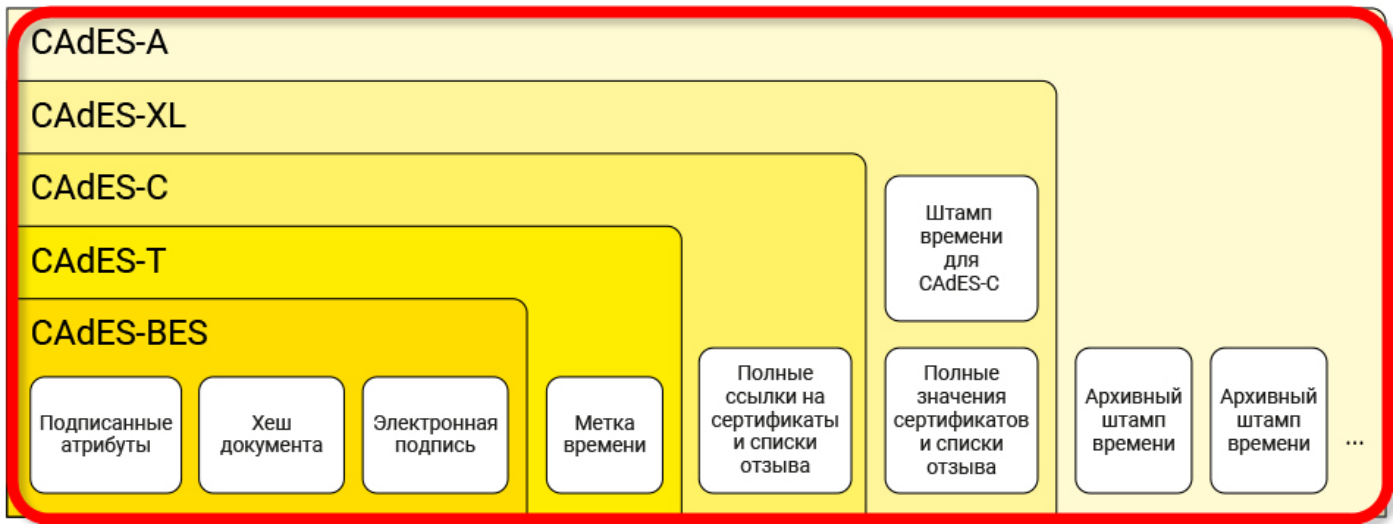


Формат CAdES-A (архивная)

- Лучше всего подходит для долгосрочного хранения документов
- Хранит подписанную информацию об отзывах
- Защищает от устаревания алгоритмов подписи
- Может занимать много места (зависит от размера списков отзыва, которые могут занимать десятки мегабайт, увеличивая размер файла подписи)

Что выбрать при подписании?

- **Самый надежный вариант – это CAdES-A. Такая подпись содержит максимальное количество информации для обеспечения успешной проверки в любой момент.**



Что выбрать при подписании?

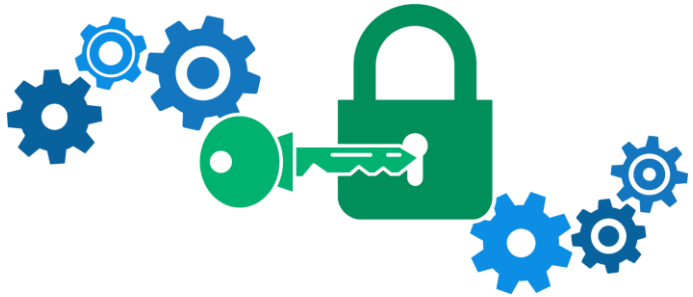
- Самый надежный вариант – это CAdES-A, но стоит учитывать
  - **Размер дискового пространства**
  - CAdES-A может занимать на порядок больше места, чем другие варианты.
  - Зависит от размера CRL конкретного удостоверяющего центра
  - Могут быть ситуации, когда CAdES-BES занимает единицы килобайт, а при усовершенствовании до CAdES-A размер увеличивается до десятков мегабайт

Что выбрать при подписании?

- Самый надежный вариант – это CAdES-A, но стоит учитывать
  - **Доказательства подлинности, не входящие в ЭП**
  - При необходимости доказать подлинность подписи можно использовать не только сам файл ЭП, но и другую информацию.
  - Например, ФНС присылает квитанции о принятии отчетности, которые могут служить доказательством, в том числе после истечения срока сертификата.
  - В регламенте использования УНЭП может быть прописано хранение дополнительных данных об ЭП (дата подписания, сведения об отзывах сертификатов) особенным образом, без включения этой информации в файл ЭП. Этот регламент может быть прописан в соглашении между участниками документооборота.

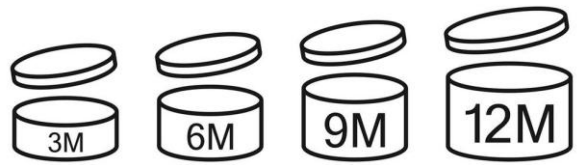
Что выбрать при подписании?

- Самый надежный вариант – это CAdES-A, но стоит учитывать
  - **Алгоритмы ЭП**
  - TSP-службы, указанные в типовых конфигурациях по умолчанию, на текущий момент поддерживают только алгоритмы ГОСТ. При получении метки для ЭП с другими алгоритмами будет выдана ошибка.
  - Для УНЭП могут использоваться другие алгоритмы. Важно убедиться, что TSP-службы, указанные в настройках, их поддерживают. Иначе можно будет использовать только подписи без меток, т.е. CAdES-BES.



Что выбрать при подписании?

- **Самый надежный вариант – это CAdES-A, но стоит учитывать**
  - **Срок хранения документа.** Если срок небольшой и риск утраты удостоверяющим центром информации о сертификатах и списках отзыва оценивается как несущественный, можно рассмотреть использование CAdES-T или даже CAdES-BES.



Что выбрать при подписании?

- Самый надежный вариант – это CAdES-A, но стоит учитывать
  - **Взаимодействие со сторонним ПО.** Не все программы и сервисы поддерживают все перечисленные форматы ЭП. Более новые форматы поддерживает меньше программ.
  - В частности, формат CAdES-A v3 не поддерживается в полной мере порталом «Госуслуги». При проверке такой подписи может быть выдан отрицательный результат, даже если ЭП сформирована в полном соответствии со спецификацией.

Что выбрать при подписании?

- **Усовершенствование – не панацея, а меньшее из зол**
- Сценарий, при котором CAdES-BES лучше, чем форматы с меткой времени:
  - Злоумышленник завладел закрытым ключом контрагента
  - Подписал документ, направил его нам
  - Контрагент заметил утечку, обратился в УЦ, сертификат отозвали
  - Мы проверяем подпись

Что выбрать при подписании?

- **Усовершенствование – не панацея, а меньшее из зол**
- Сценарий, при котором CAdES-BES лучше, чем форматы с меткой времени:
  - Злоумышленник завладел закрытым ключом контрагента
  - Подписал документ, направил его нам
  - Контрагент заметил утечку, обратился в УЦ, сертификат отозвали
  - Мы проверяем подпись

- **Для CAdES-A будет использован список отзыва из подписи, в котором еще нет сертификата. Подпись верна.**
- **Для CAdES-T список отзыва будет получен из УЦ, но тот, который действовал на дату подписания, т.е. до отзыва нашего сертификата. Подпись верна.**
- **Для CAdES-BES будет получен самый последний список отзыва из УЦ, в нем уже есть сертификат ЭП. Подпись неверна.**

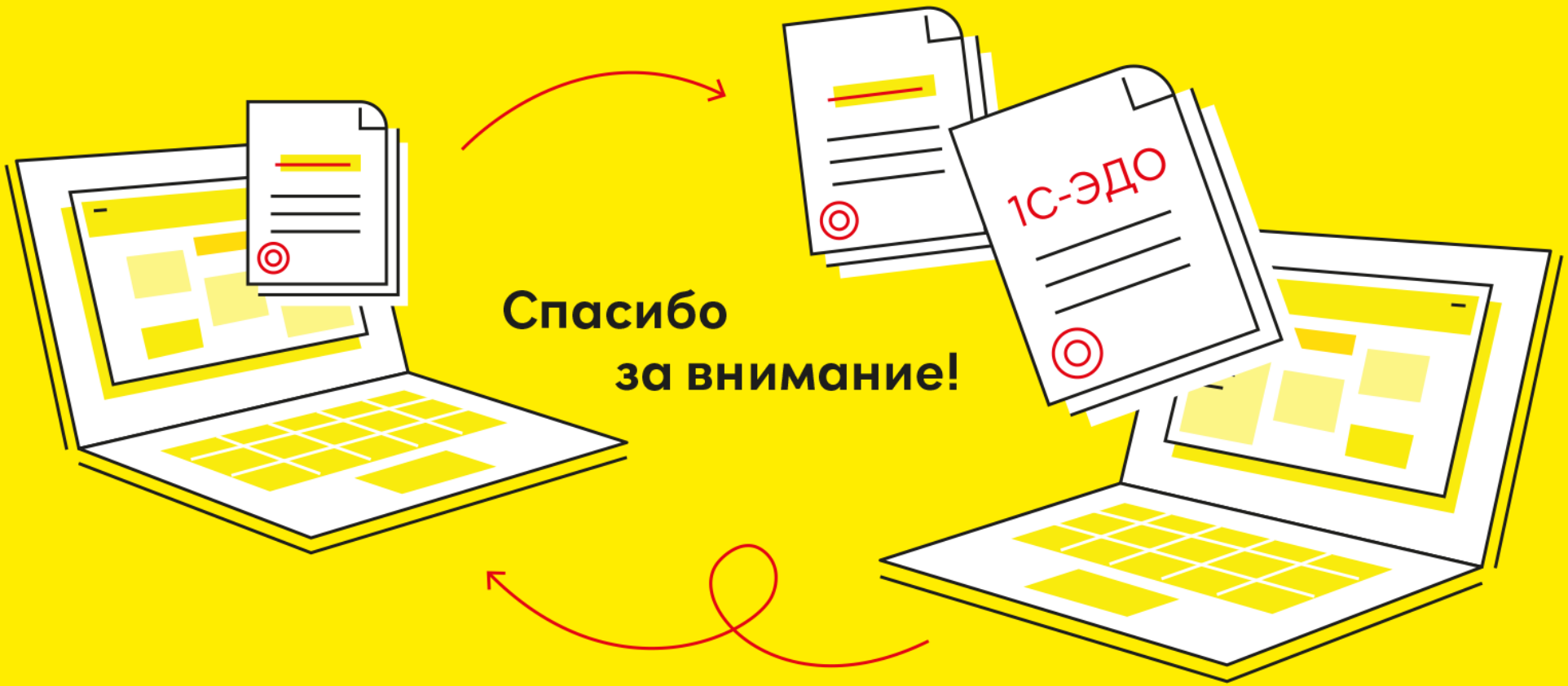
- **Технически CAdES-A и CAdES-T проверены правильно, но на практике имеем проблему**
- **Для CAdES-BES будет обратная проблема – все ЭП, сформированные до утечки, при проверке будут признаны недействительными**

Спасибо за внимание!

Как выбрать формат электронной подписи при подписании документов

03.04.2025 ★ 5 7049

При подписании документов и файлов типовые конфигурации 1С предлагают выбрать тип подписи: «Базовая», «С меткой доверенного времени», «Архивная». Эксперты 1С рассказывают, как сделать этот выбор, чем отличается УНЭП от УКЭП, что такое метка времени, CAdES, CRL, TSP и OCSP.



Спасибо
за внимание!