# Организация электронного документооборота и применение ЭЦП

Федеральное казначейство

*Зам. начальника Управления режима секретности и безопасности информации*

***Медведев***
***Анатолий Борисович***

## Обеспечение решения проблемы подлинности и юридической значимости документа

Важнейшими свойствами "генетически" сформированной рукописной подписи на документе являются:

- **Подпись достоверна**. Она убеждает получателя в том, что подписавший сознательно подписал документ.
- **Подпись неподдельна**. Она доказывает, что именно подписавший, и никто иной, сознательно подписал документ.
- **Подпись не может быть использована повторно**. Она является частью документа, мошенник не сможет перенести подпись на другой документ.
- **Подписанный документ нельзя изменить**. После того, как документ подписан, его невозможно изменить.
- **От подписи невозможно отречься**. Подпись и документ имеют материальную основу. Подписавший не сможет впоследствии утверждать, что он не подписывал документ.

# (1) Основные понятия

- **Документ** — материальный носитель с зафиксированной на нем в любой форме информацией в виде текста, звукозаписи, изображения и (или) их сочетания, который имеет реквизиты, позволяющие его идентифицировать, и предназначен для передачи во времени и в пространстве в целях общественного использования и хранения *(Федеральный закон № 77-ФЗ «Об обязательном экземпляре документов» от 23.11.1994 г. (с изменениями, внесенными Федеральным законом от 26.03.2008 N 28-ФЗ)*
- **Электронный документ** – документ, в котором информация представлена в электронно-цифровой форме *(Федеральный закон от 10.01.2002 №1-ФЗ «Об электронной цифровой подписи»)*
- **Электронная цифровая подпись** – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе *(Федеральный закон от 10.01.2002 №1-ФЗ «Об электронной цифровой подписи»)*

# (2) Основные понятия

- **Сертификат ключа подписи** - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи *(Федеральный закон от 10.01.2002 №1-ФЗ «Об электронной цифровой подписи»)*.

- **Владелец сертификата ключа подписи** - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы) *(Федеральный закон от 10.01.2002 №1-ФЗ «Об электронной цифровой подписи»)*

# Электронная цифровая подпись (ЭЦП)

## Основные угрозы системе электронного документооборота

- нарушение целостности ЭД;
- нарушение неотказуемости ЭД;
- нарушение адекватности отображения ЭД.

**Реализация угроз может привести к ряду конфликтов между участниками электронного документооборота:**

- отказ от факта приема (получения) или передачи (отправки) ЭД;
- опротестование содержания и/или времени приема или передачи ЭД;
- отказ от авторства ЭД.

**Решение:**

Использование ЭЦП в системе электронного документооборота

# Требования к ЭЦП

**ЭЦП должна:**

- подтверждать, что подписывающее лицо не случайно подписало электронный документ;
- подтверждать, что только подписывающее лицо, и только оно, подписало электронный документ;
- должна зависеть от содержания подписываемого документа и времени его подписания.
- подписывающее лицо не должно иметь возможности в последствии отказаться от факта подписи документа.

# Условия признания равнозначности ЭЦП собственноручной подписи:

Одновременное соблюдении следующих условий:

1) Сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа
2) Наличие доказательств, определяющих момент подписания;
3) Подтверждена подлинность электронной цифровой подписи в электронном документе;
4) Электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

## Криптография с симметричными ключами:

Отправитель и получатель сообщений используют один и тот же (общий) ключ (секретный элемент), как для шифрования, так и для расшифрования.

**Преимущества:**

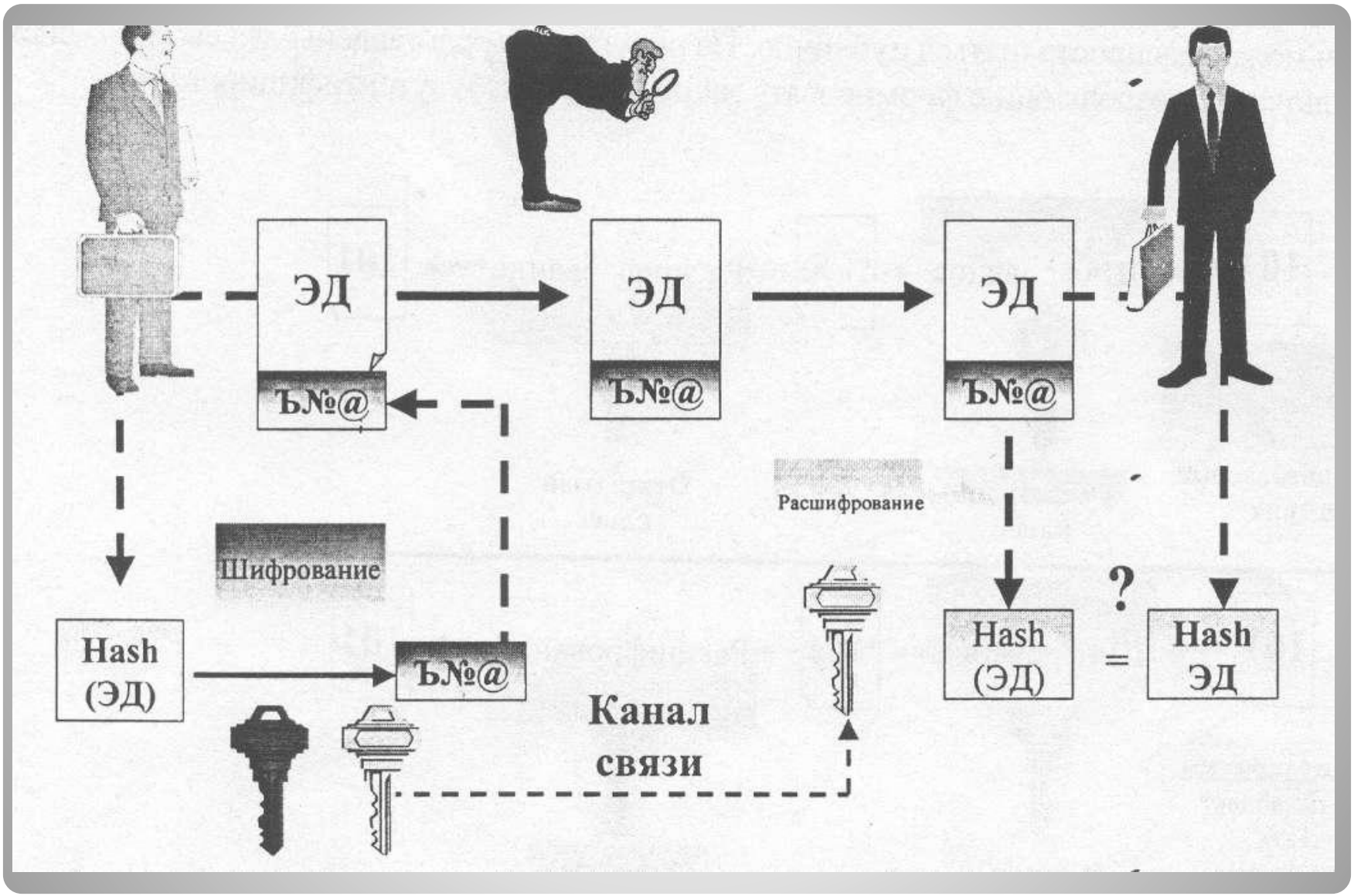
- относительно высокая производительность алгоритмов;
- высокая криптографическая стойкость алгоритмов на единицу длины ключа.

**Недостатки:**

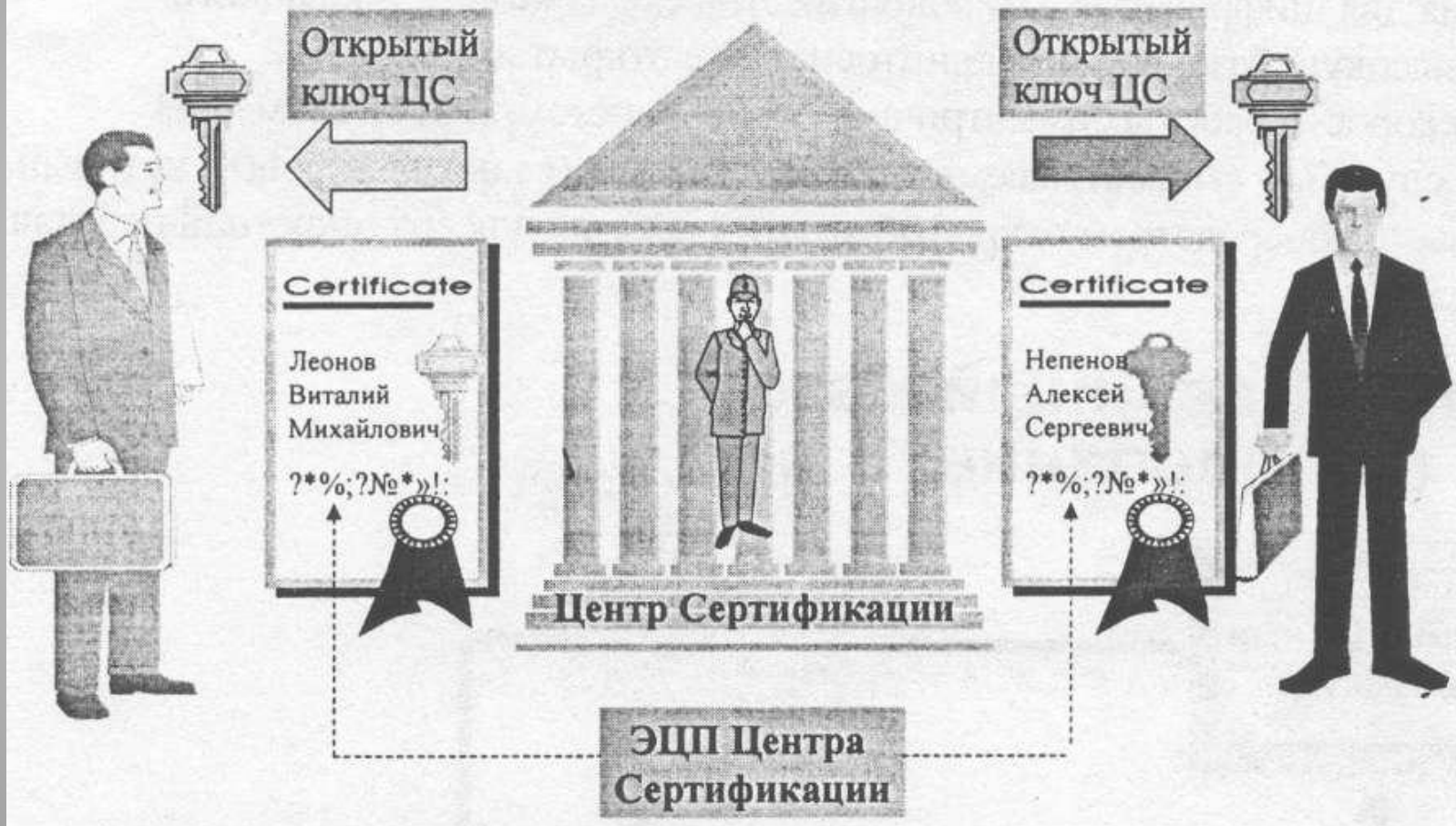
- необходимость использования сложного механизма распределения ключей;
- технологические трудности обеспечения неотказуемости.

## Криптография с открытыми ключами

Используется пара ключей: открытый (публичный) ключ и секретный (личный, индивидуальный) ключ, известный только одной взаимодействующей стороне


ЭД
ЪЬ№@
ЭД
ЪЬ№@
ЭД
ЪЬ№@
Расшифрование
Шифрование
Hash (ЭД)
ЪЬ№@
Канал связи
Hash (ЭД)
?
=
Hash ЭД

# Взаимодействие клиентов с Центром Сертификации



**В соответствии с законом "Об ЭЦП" цифровой сертификат содержит следующие сведения:**

- уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;
- фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима удостоверяющим центром вносится запись об этом в сертификат ключа подписи;
- открытый ключ ЭЦП;
- наименование средства ЭЦП, с которым используется данный открытый ключ ЭЦП;
- наименование и местонахождение удостоверяющего центра, выдавшего сертификат ключа подписи;
- сведения об отношениях, при осуществлении которых электронный документ с ЭЦП будет иметь юридическое значение.

# Формирование и проверка ЭЦП

1.Проверка сертификата с помощью открытого ключа ЦС. 2.Импорт открытого ключа отправителя. 3. Проверка ЭЦП отправителя


В рамках S\MIME (Secure Multipurpose Internet Mail Extension) подписанное ЭЦП сообщение содержит сертификат

# Электронный сертификат

**Сертификаты открытых ключей (в электронном виде)** - это структуры данных, предназначенные для хранения, распространения или пересылки по незащищенным каналам открытых ключей с гарантией их целостности и аутентичности (принадлежности конкретным субъектам).

**Раздел данных** - содержит открытые данные включающие, как минимум, открытый ключ и идентифицирующую сторону информацию (имя объекта и дополнительные сведения).

- **Пользовательское имя** в формате отличительного имени (DN). DN определяет название пользователя, и любые дополнительные атрибуты, требуемые для уникального идентификатора пользователя (например, DN может содержать пользовательский номер служащего).
- **Открытый ключ пользователя**. Открытый ключ требуется для того, чтобы пользователи могли реализовать услуги по защите информации через использование открытых ключей в сертификате.
- **Период действия** (или срок службы) сертификата (начальная и конечная даты).

**Дополнительная информация** может включать:

- **срок действия открытого ключа**;
- **серийный номер** или имя, идентифицирующее сертификат или ключ;
- **дополнительную информацию о владельце сертификата** (например, обычный или сетевой
- адрес);
- **дополнительную информацию о ключе** (например, алгоритм и намечаемое использование);
- **особые характеристики**, относящиеся к идентификации представляемого объекта, генерированию ключевой пары или к другим проблемам политики;
- **информацию, облегчающую проверку подписи** (например, идентификатор подписывающего алгоритма, и выданное CA имя);
- **конкретные операции, для которых должен использоваться открытый ключ** (шифрования данных или ЭЦП).

**Раздел подписи** - состоит из цифровой подписи органа сертификации под разделом данных.

При издании сертификата осуществляется подписание раздела данных центром сертификации.

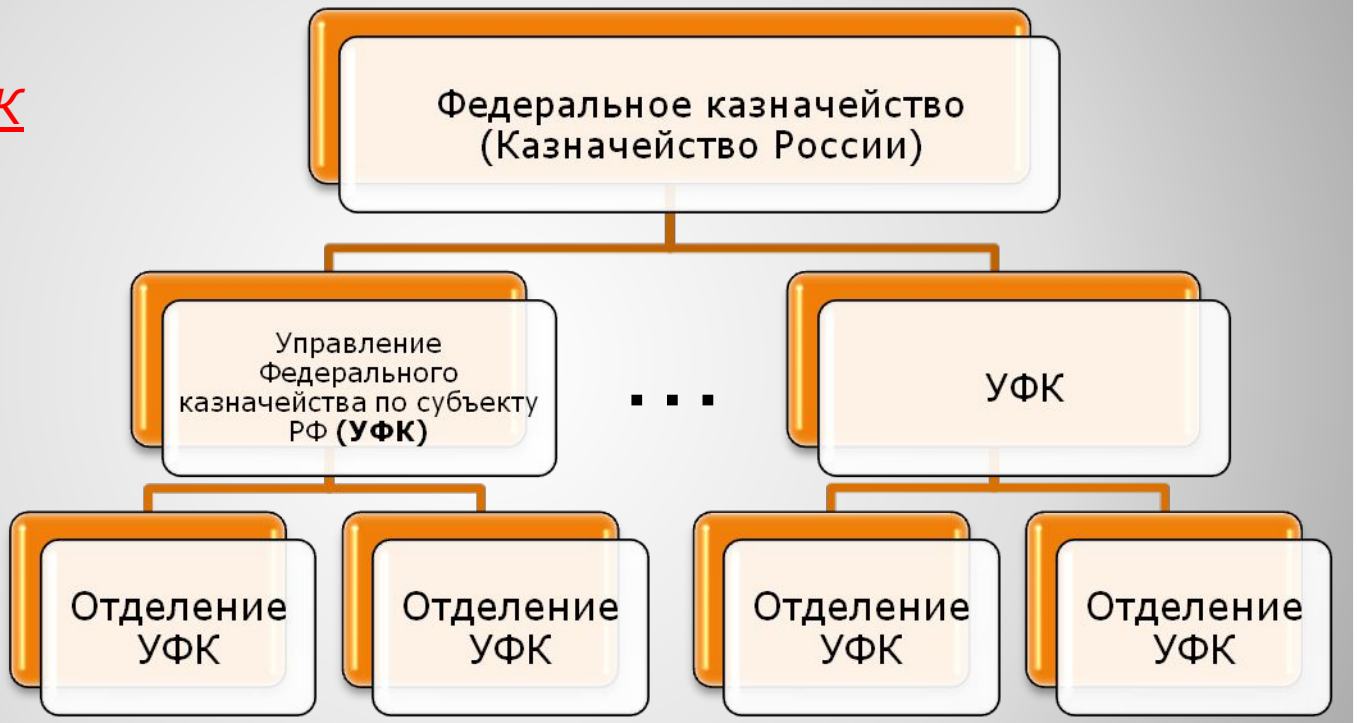
Издавая сертификат, издатель удостоверяет подлинность (дает свои гарантии подлинности) связи между открытым ключом субъекта и идентифицирующей его информацией.

# Структура Федерального казначейства

*Уровень ЦА ФК*

*Уровень УФК*

*Уровень ОФК*

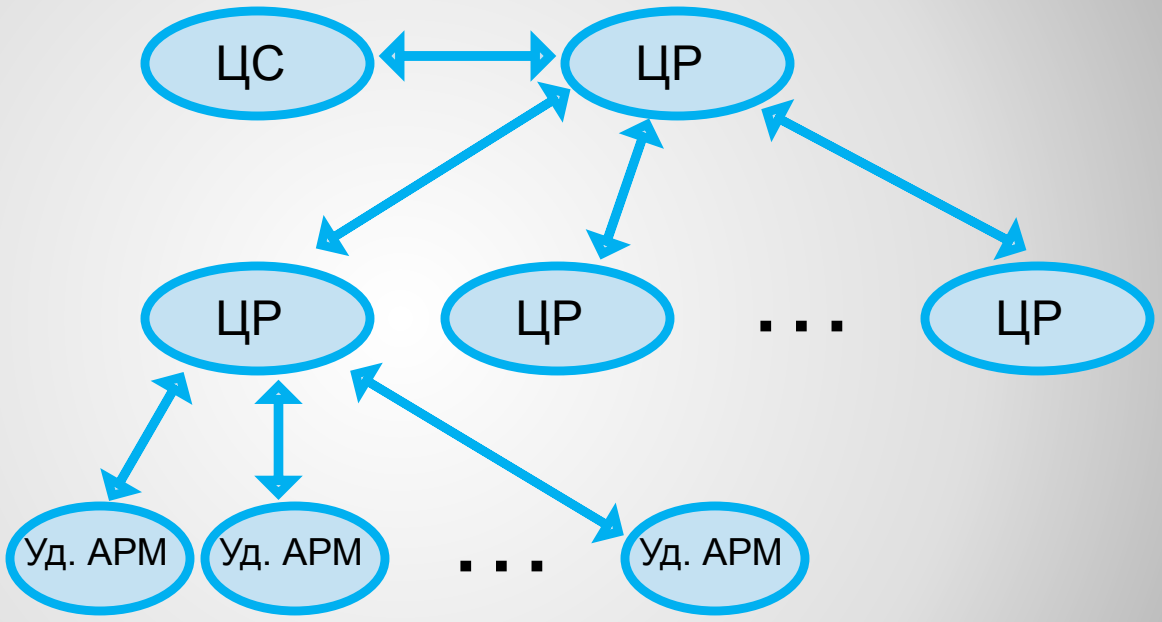


# Инфраструктура открытых ключей Федерального казначейства

*Уровень ЦА ФК*

*Уровень УФК*

*Уровень ОФК*



# (1) **Основные этапы подключения к СЭД ФК**

I. Заключение договора об обмене ЭД.
- «Типовой договор об обмене ЭД»

II. Передача Клиенту ПО и СКЗИ.
- «ППО СЭД»;
- СКЗИ (Средство ЭЦП) «КриптоПро CSP»;
- СКЗИ «Континент-АП» (включая ключи и сертификаты аутентификации);
- Эксплуатационная документация.

III. Техническое подключение к СЭД ФК
- Проведение технических мероприятий по подключению к СЭД органа ФК;
- Подписание акта готовности к обмену.

# (2) **Основные этапы подключения к СЭД ФК**

IV. Генерация запроса на сертификат открытого ключа ЭЦП.

- Запрос на сертификат (в электронном виде на машинном носителе);
- Заявление (заявка) на получение сертификата;

V. Регистрация Клиента в ЦР УУЦ ФК

- Приказ организации Клиента о назначении уполномоченных лиц;
- Запрос + Заявка на поолучение сертификата;
- Удостоверяющие документы соискателя сертификата (или доверенность).

## (3) **Основные этапы подключения к СЭД ФК**

VI. Сертификация ОК ЭЦП Клиента.

- Проверка соответствия запроса на сертификат заявке на получение сертификата;
- Утверждение запроса на сертификат;
- Направление запроса на сертификацию в ЦС УУЦ ФК.

VII. Передача сертификата ОК ЭЦП клиента и корневого сертификата.

- Передача клиенту сертификата ОК ЭЦП Клиента и корневого сертификата ЦС УУЦ ФК (запись на машинный носитель, дистанционная установка на рабочую станцию Клиента в СЭД ФК)

VIII. Установка сертификатов на РС.

# Особенности организации работы с сертификатами УУЦ ФК на ЭТП