Аутсорсинг электронной подписи

Уральский форум, 2015

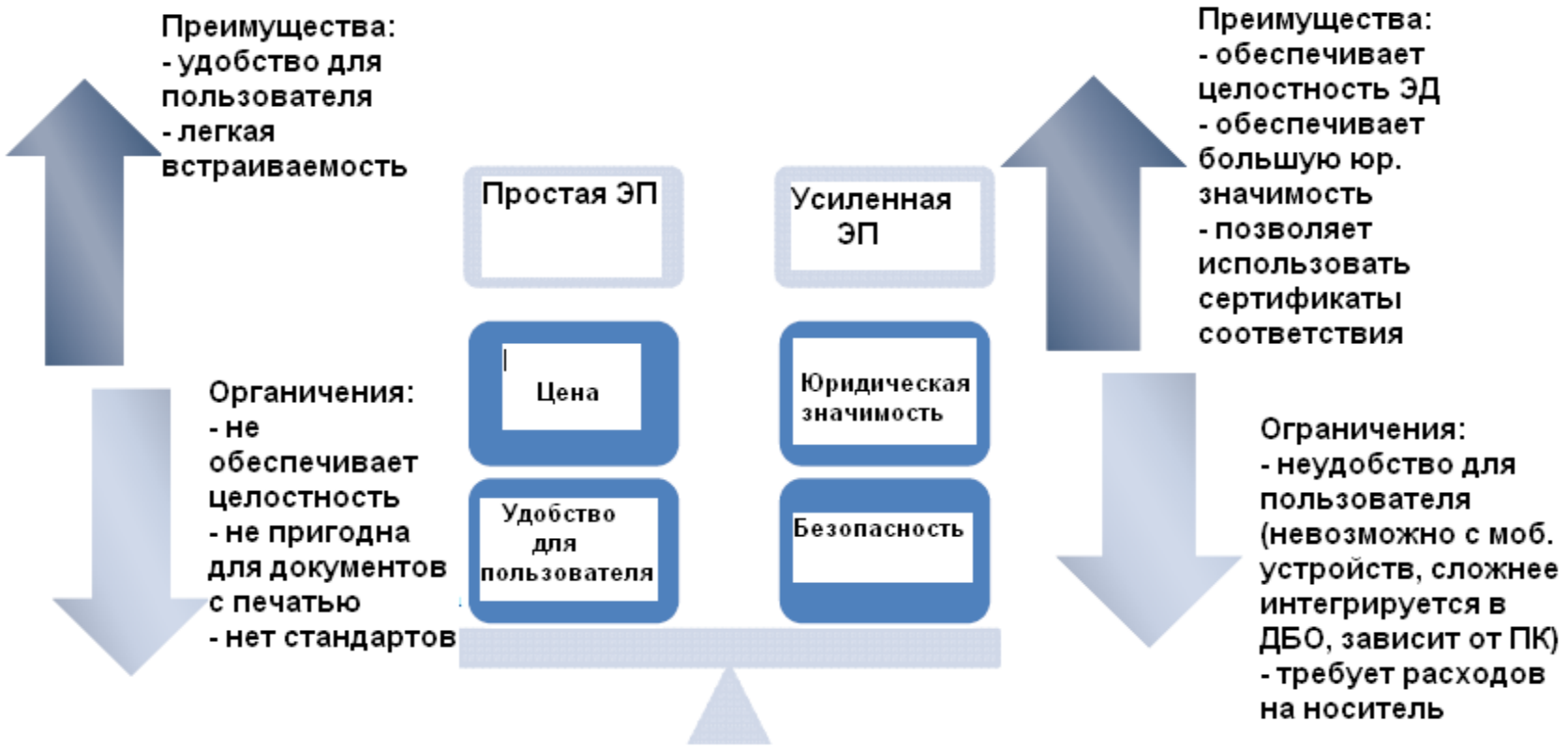
Янсон И.А.

План презентации

1. Простая и усиленная ЭП в ДБО
2. Проблемы применения усиленной ЭП в ДБО
3. Понятие облачной ЭП
4. Компоненты облачной ЭП
5. Основные функции облачной ЭП. Схема подписания ЭД облачной ЭП
6. Облачная ЭП в контексте 63-ФЗ – это вид усиленной ЭП
7. Сравнение «традиционной» и облачной ЭП
8. Сравнение корпоративного и аутсорсингового вариантов внедрения

Простая и усиленная ЭП в ДБО

Соотношение между простой и усиленной электронной подписями при использовании в системах ДБО



Проблемы применения усиленной ЭП в ДБО

Использование усиленной ЭП в ДБО обычно означает, что в системе используется **СКЗИ** и у пользователя есть **закрытый ключ ЭП**, который должен быть доступен только его владельцу. Чаще всего для хранения ключа ЭП используется защищенный носитель в формате USB-токена или смарт-карты. СКЗИ устанавливается или на устройство пользователя, или оно может быть на том же носителе, где хранится ключ.

Наличие **СКЗИ и защищенного носителя** порождает **следующие проблемы**:

- **Проблемы использования на мобильных устройствах**

  - Усиленная подпись требует использования СКЗИ. Внедрение СКЗИ в мобильные приложения приводит к тому, что мы начинаем распространять вместе с мобильными приложениями и СКЗИ через интернет-магазины приложений (iTunes AppStore, Google Play, Windows Store)

  - Для обеспечения безопасности необходимо хранить закрытый ключ ЭП на защищенном носителе. На мобильных устройствах это сложно обеспечить. Особенно если есть требование по возможности работы с разных устройств.

- **Проблемы трансграничного использования**

  - нельзя вывозить ПК с СКЗИ или токены/смарткарты с СКЗИ заграницу

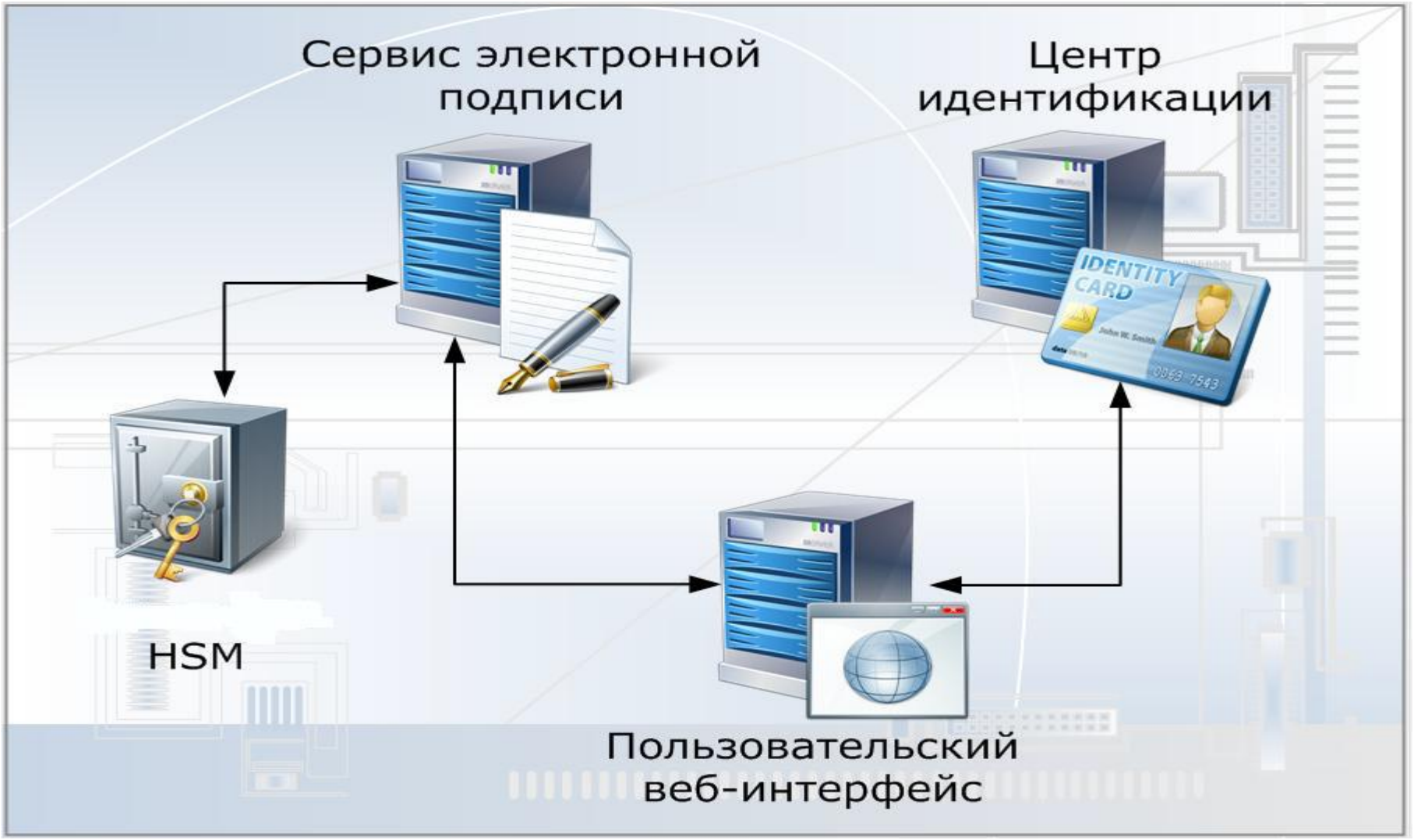
Понятие облачной ЭП

Облачная электронная подпись – это вычислительная система, предоставляющая через сеть доступ к возможностям создания, проверки ЭП и интеграции этих функций в бизнес-процессы других систем.

Облачная ЭП как система состоит из:

- Аппаратного криптографического модуля (Hardware Security Module)
  - используется для формирования ключей ЭП, для выработки ЭП для ЭД, для хранения ключей ЭП (опционально)
- Центра идентификации
  - используется для аутентификации пользователя и платежей
- Сервиса электронной подписи
  - содержит интерфейс для обращения приложения пользователя, может хранить ключи ЭП (в зашифрованном виде)
- Интерфейса для обращения пользователя (приложения пользователя)
  - используется при интерактивной работе пользователя

Компоненты облачной ЭП



Основные функции облачной ЭП

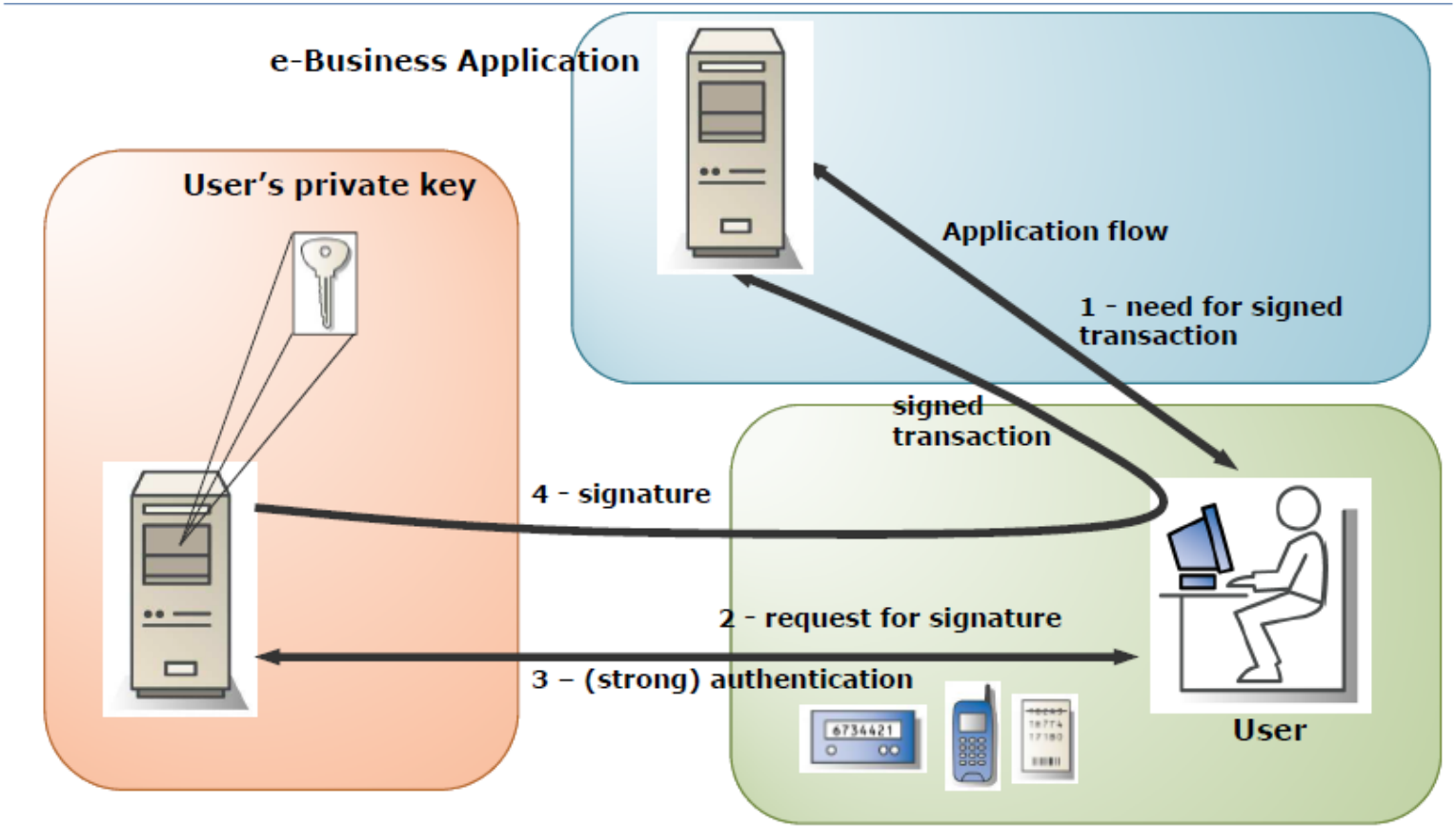
Генерация ключей:

1. Пользователь обращается к серверу ЭП, указывая PIN-код
2. Сервер обращается к HSM с просьбой сформировать ключ ЭП и PIN-код
3. HSM возвращает Серверу ЭП ID для ключа
4. Сервер ЭП связывает пользователя с ID его ключа ЭП

Формирование подписи:

1. Пользователь обращается к приложению (например, ДБО), формирует в нем ЭД
2. Приложение обращается к серверу ЭП, передает ему документ для подписи
3. Сервер ЭП аутентифицирует пользователя
4. Сервер ЭП передает в HSM PIN-код к ключу ЭП и ЭД на подпись
5. HSM формирует электронную подпись для ЭД и возвращает ее на сервер ЭП
6. Сервер ЭП передает подписанный ЭД в приложение пользователя

Схема подписания ЭД облачной ЭП



Согласно закону 63-ФЗ «Об электронной подписи»

Статья 5. Виды электронных подписей

3. Неквалифицированной электронной подписью является электронная подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи.

Статья 10. Обязанности участников электронного взаимодействия при использовании усиленных электронных подписей

При использовании усиленных электронных подписей участники электронного взаимодействия обязаны:

1) обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;

2) уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

3) не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

Требования 63-ФЗ к усиленной ЭП

Статья 12. Средства электронной подписи

1. Для создания и проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи должны использоваться средства электронной подписи, которые:

1) позволяют установить факт изменения подписанного электронного документа после момента его подписания;

2) обеспечивают практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки.

2. При создании электронной подписи средства электронной подписи должны:

1) **показывать** лицу, подписывающему электронный документ, **содержание информации**, которую он подписывает;

2) **создавать электронную подпись только после подтверждения** лицом, подписывающим электронный документ, операции по созданию электронной подписи;

3) однозначно показывать, что электронная подпись создана.

3. При проверке электронной подписи средства электронной подписи должны:

1) показывать содержание электронного документа, подписанного электронной подписью;

2) показывать информацию о внесении изменений в подписанный электронной подписью электронный документ;

3) указывать на лицо, с использованием ключа электронной подписи которого подписаны электронные документы.

Облачная ЭП – это вид усиленной ЭП

1)Очевидно, что требования статей 5 (часть 3), 10, 12 (часть 1) выполняются

2)Требования ст.12 часть 2,3

2. Ст. 12 "Средства электронной подписи",

п. 5 "Требования частей 2 и 3 настоящей статьи не применяются к средствам электронной подписи, используемым для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе."

•Так как облачная подпись формируется на сервере, то потенциально можно говорить, о том, что облачная подпись создается автоматически. Если это верно, тогда можно говорить о том, что для облачной ЭП не требуется выполнения частей 2,3 п.5 статьи 12, то есть выполнения требований к средствам формирования и проверки ЭП отображать документ, показывать, что подпись создана и т.д.

•С другой стороны при создании облачной ЭП под ЭД проводится аутентификация пользователя и действий по подписанию ЭД. Например, путем отправки подтверждающего СМС-кода. В случае если СМС-код пересылается с реквизитами платежа, то можно говорить о том, что требование части 2 п.5 статьи 12 все же выполняется.

•Если же говорить о традиционной ЭП с использованием USB-токенов/смарткарт, то в этом случае подписание точно не является автоматическим, а требования частей 2,3 п.5 статьи 12 точно не выполняются.

Вывод: Облачная ЭП является полноценной усиленной ЭП

Сравнение «традиционной» и облачной ЭП: обеспечение защиты

	Усиленная ЭП на смарткарте	**Усиленная ЭП на сервере ЭП**
Защита закрытого ключа ЭП от копирования	Обеспечивается (неизвлекаемое хранение)	Обеспечивается (неизвлекаемое хранение)
Защита от подписания ЭД путем удаленного управления ключом ЭП	Требует дополнительных средств (например, визуализации документа)	По умолчанию достигается, так как подпись требует аутентификации
Защита от подмены ЭД при подписи (автозалив)	Требует дополнительных средств (например, визуализации документа)	По умолчанию достигается, так как подпись требует аутентификации
Защита закрытого ключа ЭП от кражи/утери	Защитить невозможно	Кража/утеря невозможна. Возможно организовать бэкапирование.

Сравнение «традиционной» и облачной ЭП: удобство использования

	Усиленная ЭП на смарткарте	**Усиленная ЭП на сервере ЭП**
Возможность использования на мобильных устройствах	Затруднена	Обеспечивается
Возможность использования клиентами в офисе банка	Сопряжена с определенными сложностями (сложнее настройка, СКЗИ).	Достаточно иметь простой интернет киоск.
Возможность разделения носителя между пользователями	Запрещена, так как приводит к компрометации ЭП	Не требуется приобретать носитель для каждой ЭП.

Сравнение «традиционной» и облачной ЭП: сопровождение сертификатов/ключей

	Усиленная ЭП на смарткарте	**Усиленная ЭП на сервере ЭП**
Продление сертификата	Требует личного визита пользователя в офис и ручных действий сотрудника Банка	Может быть решено дистанционно. Делается быстрее и проще.
Перевыпуск ключа ЭП		
Забытый PIN-код		

Сравнение «традиционной» и облачной ЭП: требования, связанные с СКЗИ

	Усиленная ЭП на смарткарте	**Усиленная ЭП на сервере ЭП**
Необходимость наличия лицензии ФСБ	Требуется лицензия на распространение, на встраивание	На распространение не требуется. Если аутсорсинг, то и встраивания нет.
Обученный по теме СКЗИ персонал	Требуется всегда	При аутсорсинге не требуется. При in house использовании только в ГО.
Возможность использования заграницей	Проблематично, так как возникает экспорт СКЗИ	Нет никаких ограничений

Сравнение «традиционной» и облачной ЭП: стоимость, интеграция, аудит

	Усиленная ЭП на смарткарте	Усиленная ЭП на сервере ЭП
Стоимость	Выше, так как для каждой ЭП нужен носитель	Не требуется приобретать носитель для каждой ЭП.
Удобство развертывания, интеграции	Требует встраивания СКЗИ, затруднено на мобильных устройствах	Интеграция обеспечивается достаточно просто
Аудит	Обращения к ключам ЭП журналируются неполностью.	Все события, связанные с использованием ключей ЭП журналируются

Новые требования

При использовании облачной подписи возникают следующие специфические требования:

1. Защита ключей ЭП от неавторизованных пользователей/процессов
2. Обеспечение доступности аутентификационной информации только пользователю ключа ЭП
3. Обеспечение высочайшего уровня отказоустойчивости сервиса, так как от его работоспособности зависит работа соответствующего приложения (например, системы ДБО)
4. Защита от риска отказа пользователя от своей подписи
5. Если сервис оказывается третьей стороной, то требуется наличие доверия к этой третьей стороне

Кроме того, по сравнению с традиционным вариантом ключа ЭП на USB-токене/смарткарте пользователь ограничен в использовании ключа ЭП только теми приложениями, с которыми есть интеграция у сервиса облачной подписи

Сравнение аутсорсинга и собственного сервиса облачной подписи

наименование	Собственный сервис	Аутсорсинг
Лицензии сервера ЭП	Разовый расход	-
HSM		
Оборудование (серверы, сетевое оборудование и т.д), общестистемное ПО		
Сопровождения/год		
Сопровождение лицензий сервера ЭП	Постоянные платежи	-
Сопровождение оборудования и общесистемного ПО		
Штатные единицы поддержки сервера ЭП, HSM, средств защиты (уровень поддержки 24X7)	Постоянные платежи	-
Стоимость выпуска сертификата		
Сервис ЭП	-	Зависит от числа пользователей
Сервис выпуска ключей	Зависит от наличия УЦ	Зависит от числа пользователей

Сравнение аутсорсинга и собственного сервиса облачной подписи

Выводы:

- Облачная ЭП по сравнению с «традиционной» ЭП является мультиканальной, легче интегрируется, удобнее для пользователей
- При больших объемах пользователей целесообразно использовать собственный сервис облачной ЭП
- Аутсорсинг облачной ЭП выгоден:
  - При небольшом числе пользователей
  - Если необходимо использование ЭП в большом числе приложений/сервисов (при условии, что есть аутсорсер, имеющий интеграцию с ними)
  - В случае, если затруднительно разместить оборудование или нанять специалистов для обеспечения 24x7 функционирования и поддержки