Вопросы и ответы с вебинара «КриптоПро DSS/myDSS. Реализация облачной электронной подписи на ПК и мобильных устройствах» от 19.06.2019 г.

1. Биометрию же тоже подтверждать нужно через какое-то время?
Да, все верно.

2. Удовлетворяет ли требованиям п.5.1 683-П технология PayControl?
683-П на данный момент вызывает много вопросов. В текущей трактовке, согласно пункту 5.1. 683-П: «Кредитные организации должны обеспечивать подписание электронных сообщений способом, позволяющим обеспечить целостность и подтвердить составление указанного электронного сообщения уполномоченным на это лицом». PayControl это реализует, но на западных криптоалгоритмах. Таким образом, PayControl – это "усиленный" ПЭП, обеспечивающий контроль авторства и целостности. 683-П, в явном виде, не запрещает использования ПЭП, если соблюдены иные условия.

3. По 63-ФЗ владелец должен обеспечить конфиденциальность ключа ЭП, в этой связи, есть ли необходимость Аттестации DSS по требованиям ФСТЭК, например, 1Г?
Предпринятые в HSM и DSS меры защиты обеспечивают конфиденциальность ключей, в т.ч., от администраторов данного ПАК. Это проверялось и обосновывалось при сертификации. Прямого требования по аттестации нет, мы со своей стороны рекомендуем это делать.

4. Можно ли использовать mydss полностью в своем фронте? без вашего мобильного приложения?
На данный момент для КЭП нельзя, но есть вариант использования для НЭП со встраиванием myDSS SDK в другое мобильное приложение.

5. В случае облачной подписи гарантом соблюдения пункта 1 статьи 10 63 ФЗ является владелец DSS?
Да.

6. Как обходится ограничение на 10 000 ключей пользователей в DSS?
Если речь об ограничении в 10000 ключей на один HSM, то DSS может хранить ключи не в HSM, а в своей БД в зашифрованном виде. Шифрование ключа осуществляется на мастер-ключе, хранимом в HSM, таким образом в незащищённом виде ключ пользователя по-прежнему не появляется вовне оперативной памяти HSM.

7. Когда ориентировочно планируется законодательное принятие удаленной идентификации для удостоверяющих центров? Есть ли какие-то ориентировочные сроки?
Скажем так, есть вероятность, что в этом году будет принят соответствующий закон.

8. Удостоверяющий центр аннулирует сертификат ключа проверки электронной подписи в следующих случаях:

1) не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи
Нет ли тут юридического противоречия, ведь ключ ЭП лежит в ХСМ и владение в полной мере нет или я не прав?
По нашему мнению, противоречия нет. Это общая норма, "буква закона" здесь говорит о п.1.1 ст.13, где оговорена процедура подтверждения владения, которую должен осуществлять УЦ. При этом другая норма, в данном случае частная по отношению к первой, разрешает использовать ключ с согласия владельца. Очевидно, нельзя использовать ключ с согласия владельца, при этом оставив владение ключом за владельцем (извините за тавтологию) "в полной мере". Поэтому частная норма в данном случае превалирует.

9. Ответственность за хранение ключей ЭП пользователей, их учету в журналах и все остальное по ФАПСИ 152, как я понимаю, будет на УЦ? Где-то в законопроектах подобное видел вроде
В обсуждаемых поправках к 63-ФЗ именно так. Только про ответственность за хранение, не про учёт по ФАПСИ-152 и т.п.

Но ведь хранение подразумевает и учет. Неизвестно как при проверках на это посмотрят. Надо уточнить этот вопрос с регулятором (может информационное письмо
опубликовать?)
Согласны с вами. Если есть сомнения, надо уточнять у регулятора. Но это вопрос не к 63-ФЗ.

10. Какая документация должна быть разработана при использовании DSS+HSM в удостоверяющем центре?
Зависит от способа применения и круга лиц, хранящих ключи в DSS+HSM.

выдача квалифицированных ЭП клиентам с хранением ключей в DSS
Как минимум, необходимо расширить комплект заявительных документов, который будущий владелец сертификата подает в удостоверяющий центр для включения соответствующего поручения на создание ключа и его распоряжению. Этот момент описан в документах Правилах пользования DSS.

11. Как подключить DSS к АУЦ, можно поподробнее?
Сейчас нет сертифицированных средств УЦ, доступных на рынке, которые можно подключать к сетям общего пользования. Соответственно, если DSS "смотрит" в Интернет, то к АУЦ в онлайн он подключен быть не может. Запросы на сертификат и выданные сертификаты туда-сюда можно переносить в виде файлов через "воздушный зазор".

12. Что значит "передача безопасным способом запроса на сертификат"?
Передача запросов на сертификат и выданных сертификатов в виде файлов через "воздушный зазор". (взаимодействие DSS с АУЦ)

13. Автоматический выпуск сертификатов из DSS в АУЦ допустим ли в соответствии с требованиями эксплуатационной документации на УЦ 2.0?
Автоматический выпуск вряд ли возможен через "воздушный зазор", поэтому нет. См. мой ответ выше (11 и 12). Если под "автоматическим выпуском" имеется в виду что-то другое, то прошу пояснить вопрос.

Может тут можно конечно использовать криптомаршрутизатор сертифицированный по КВ?
Работы в этом направлении ведутся.

14. При использовании DSS необходимо ли иметь лицензию на ТЗКИ, или лицензии ФСБ достаточно?
DSS - это СКЗИ, сертифицированное ФСБ и подпадает на наш взгляд только под регулирование ФСБ, в том числе в части лицензирования деятельности.

15. Зачем NGate в DSS? Он заменяет сервер аутентификации из состава DSS?
NGate здесь опционален. Он может повысить защищённость подключения к DSS и снять часть нагрузки по TLS с сервера DSS.

16. Когда ориентировочно ожидать сертификат соответствия на CSP 5? Его отсутствие сдерживает внедрение...
Ожидаем в середине июля. Отмечу, что формально по букве ПКЗ-2005 СКЗИ можно эксплуатировать после получения положительного заключения.

17. На демонстрации входа на сайт госуслуги использовался режим аутентификации по паролю? а где же myDSS???
Демонстрировался вход "по электронной подписи", ключ которой хранится в DSS. Делается с использованием технологии "Cloud CSP". Можно то же самое проделать и с myDSS, в демонстрации он не был настроен.

18. При выводе формы аутентификации для использования закрытого ключа в CloudCSP какой TLS|SSL нужно применять? По RSA подойдет? при использовании квалифицированной ЭП?
Те же самые требования, как и для подключения к веб-интерфейсу DSS. Если подписываемый документ показывается в myDSS, то можно и RSA TLS.

19. Возможно ли использовать КриптоПро CSP 5 для работы с усиленными квалифицированными СКПЭП? В выписке из заключения нет отсылки к 63-фз или 795 приказу ФСБ.
Да. CSP 5.0 сертифицировался одновременно и как СКЗИ и как средство ЭП по соответствующим требованиям. В сертификате ФСБ об этом будет.

20. Подскажите, а с помощью КриптоПро эцп браузер плагина и csp 5.0 можно сформировать ключи в дсс и отправить запрос в уц?
В настоящий момент создание ключа в DSS через Cloud CSP невозможно. Планируем сделать в будущем.

21. При использовании КриптоПро CSP 5.0 и аутентификации пользователя по логину/паролю центр идентификации DSS и пользователь должны быть в одном сегменте сети или возможен доступ через Интернет?
Если только по логину/паролю, то только в одном сегменте.

22. Правильно я понимаю, что Крипто Про CSP 5 нельзя использовать при работе с DSS+HSM, если планируется работа с усиленными квалифицированными СКПЭП?
Можно.

23. Контроль ОС смартфона будет производиться как у Сбербанк онлайн? защита от "рутования" ОС?
Контроль производится и сейчас. Это есть в приложении.

24. Можно ли синхронизировать БД ЦР из состава УЦ с БД ЦИ?
Нельзя.

25. Что входит в отпечаток мобильного устройства?
Набор уникальных признаков аппарата (доступные серийные номера железа, коды производителей и пр.) + случайная последовательность, уникальная для экземпляра приложения.

26. Как происходит визуализация в mydss? пользователь может скачать документ?
Да, myDSS позволяет визуализировать либо текст, либо PDF-документ.
DSS может выполнять конвертацию из разных форматов (например, docx или сканы TIFF) в PDF перед отправкой на подтверждение в мобильное приложение.

27. Будет ли реализован графический интерфейс для развертывания DSS?
Реализация в планах есть.

28. Можно ли совмещать архитектуру УЦ И DSS? И какие компоненты можно устанавливать на одном ТС?
Для работы с квалифицированными сертификатами ПАК УЦ должен быть изолирован от DSS – в этом случае нельзя. При работе с неквалифицированными сертификатами мы не рекомендуем размещать компоненты УЦ и DSS на отдельном ТС.

29. Может ли один экземпляр myDSS на устройстве показывать скины разных банков?
Да, можно.

30. Какие документы могут быть подписаны при помощи myDSS? Если я не ошибаюсь, то раньше в документации была фраза, что допускается подписание только неконфиденциальных документов.
Да, верно. Фраза эта осталась. В будущем за счет поддержки ГОСТ TLS между серверной и клиентской компонентами myDSS можно будет подписывать конфиденциальные документы.
В настоящий момент для возможности подписания конфиденциальных документов можно использовать решение КриптоПро Ngate, к-е размещается между клиентскими и серверными компонентами myDSS.

31. Если у клиента более одного ИБК с одной подписью. Как будет работать мобильное приложение mydss? с каким скином?
Скин будет переключаться в зависимости от того, каким ключом выполняется подписание в данный момент. Само приложение (главный экран) в этом случае будет иметь "вид по умолчанию".

32. Возможна ли интеграция MyDSS с банковским моб приложением, чтобы не заморачивать клиентов скачивать еще одно приложение?
Что касается КЭП, то это в планах - мы усердно над этим работаем. Но сейчас только отдельное приложение. Для УНЭП - да, возможна. Уже сейчас.

Как?
Запросить необходимые материалы, получить SDK и выполнить интеграцию :)

А примерные сроки?
Как сказано в презентации - пока сроков нет. Как только будет ясность – обязательно сообщим всем :)

33. ГОСТ TLS как планируется реализовать?
Планируем с помощью КриптоПро CSP 5.0, который будет интегрирован в мобильное приложение myDSS.

34. DSS+myDSS - какой класс защиты?
КС1.

35. Расскажите, пожалуйста, про кластерное решение. Какие ограничения? Есть кластер из двух узлов? Используется ли какой-то отдельный центр управления кластером или его мониторинг?
Кластеризуются все компоненты: DSS / SQL / HSM.
Переключение между серверами DSS обеспечивается средствами балансировщиков.
Переключение между HSM обеспечивается средствами DSS.
Переключение между серверами SQL обеспечивается средствами AlwaysOn, FCI, SQL Mirroring и др.
Для мониторинга работоспособности можно использовать КриптоПро Центр Мониторинга.

36. Чем обусловлено рекомендуемое хранение ключей в БД вместо HSM? производительности HSM при формировании ЭП не хватает? а то ведь все старые концепции и модели ломаются))
В режиме хранения ключей в БД реализуема схема «горячего» резервирования с мгновенным переключением.

37. Есть ли ограничение на размер подписываемого файла в DSS+HSM?
Зависит от способов подписания и форматов подписи. В случае мобильного приложения myDSS можно подписать файл размером 1 Гб и более, но пользователь в таком случае должен будет загрузить этот документ, что наверняка не очень удобно.

38. Какая разница при использовании УКЭП и УНЭП в режимах эксплуатации DSS, при оказании услуг в соответствии с лицензией ФСБ другим юрлицам?
Из общих соображений, если DSS эксплуатируется для УКЭП, то необходимо выполнить все требования, указанные в эксплуатационной документации. Если DSS эксплуатируется для УНЭП можно выбирать, устраивают ли Вас и пользователей, предпринятые Вами меры защиты.

39. И еще вопрос, какое максимальное количество пользователей возможно при обоих вариантах хранения ключей?
В режиме хранения ключей в БД – ограничивается размерами дисков и памяти серверов.
В режиме хранения ключей в HSM – в одном HSM до 500 тысяч с возможностью масштабирования.

40. у вас макетирование планировалось в конце весны, насколько я помню
Уточните, пожалуйста, вопрос.

41. А если DSS и АУЦ в сегментах без доступа к сетям общего пользования, можно подключать?
Да, можно с ограничением. В этом случае потребуется произвести оценку влияния DSS на Аккредитованный УЦ.

42. А если использовать однонаправленные шлюзы с сертификатами ФСБ, можно подключать DSS и АУЦ?
В одну сторону можно (сертификаты и CRL). Запросы на сертификат на данный момент нельзя.

43. а если между DSS и АУЦ поставить шлюз по КВ2?
Да, можно с ограничением. В этом случае потребуется произвести оценку влияния DSS на Аккредитованный УЦ.

44. Но а что с доступом с TSP и OCSP при работе с аккредитованным УЦ? При работе с аккредитованным УЦ только CMS формат?
На данный момент документация не утверждена, поэтому вопрос комментировать не можем.

45. Если подписывается большой файл - 2 Гб, например, myDSS все равно будет визуализировать все содержимое?
Да, будет.

46. Возможно ли в кластере DSS применять 3 HSM одновременно подключенных к DSS?
Да, можно.

47. Для неАУЦ - в случае использования УЦ для собственных нужд (без оказания услуг по НЕквалам для других ЮЛ) - воздушный зазор не важен!
Делается на Ваше усмотрение, как владельца Удостоверяющего Центра.

48. Как производить интеграцию мобильного приложения Интернет-Банк с mydss?
Через Deep Link. Любое мобильное приложение может запустить процесс подписания в мобильном приложении myDSS, после чего получить результат подписания

49. Для встраивания КриптоПро DSS/mydss в лицензии ФСБ нам потребуется получать пункты для проведения встраивания СКЗИ в ДБО?
Вопрос имеет разные юридические трактовки. Мы придерживаемся того, что закон о лицензировании отдельных видов деятельности говорит о деятельности, направленный на извлечение прибыли (то лицензия ФСБ нужна). Если вы разрабатываете решение для собственных нужд, то в получении лицензии ФСБ необходимости нет.

50. При подписании через приложение возникла проблема. в связи с этим вопрос – есть ли требования к смартфонам
Требования к смартфонам есть, они описаны в документации. Если у Вас есть какие-то проблемы, обратитесь, пожалуйста, в нашу техническую поддержку. Мы попробуем помочь.

51. Можно ли отображать вложения документа + сам документ в MyDSS? Если да, то в каком формате?
Процесс подписания выглядит следующим образом. Один документ отображается в мобильном приложении. Документ передается в формате PDF.

52. Добрый день. Если УЦ закрывается, что происходит с облачными эп клиентов?
Вопрос, судя по всему, правого характера. На усмотрение Удостоверяющего Центра, исходя из регламентов и других договорных отношений.

53. Вопрос про необходимость применения сертифицированной версии DSS для неквалифицированной подписи при доступе других ЮЛ - возможно ли применять несертифицированную сборку DSS?
Возможно с оговорками, см. вопрос 41.

54. Как запросить необходимые материалы, получить SDK и выполнить интеграцию? Что для этого необходимо?
Пишите на почту, по контактам в вебинаре - все расскажем.

55. Приведите, пожалуйста, пример максимально короткого и удобного кейса получения пользователем сертификата в УЦ и помещения его в HSM для дальнейшего использования (с предварительной генерацией запроса на сертификат КЭП средствами DSS)
В случае эксплуатации DSS/УЦ одной организации пользователь предоставляет все необходимые заявительные документы для получения квалифицированного сертификата. Оператор в DSS регистрирует пользователя и формирует запрос на сертификат с дальнейшим выпуском, а также ключ myDSS.

56. При расшифровании ключа ЭП из СУБД DSS мастерключом, сам мастерключ из HSM извлекается ли в оперативную память сервера DSS?
Нет.

57. Если клиент захочет поменять телефон, возможна ли переустановка ключей на другой смартфон или потребуется снова создавать УЗ в DSS?

Технически рекомендуется делать привязку ключей к смартфону – в таком случае переустановка ключей на другой смартфон будет невозможна. В особых случаях привязку можно отключить и перенести ключ на другой смартфон.

58. Если ИС передает на подпись в DSS не сам документ, а хеш от документа (снижение нагрузки на канал передачи данных), то возможно ли в этом случае использовать myDSS для КЭП? Что при этом будет визуализироваться в my DSS?
Без дополнительных исследований ИС использовать так КЭП нельзя.

59. Сколько по времени занимает оценка влияния DSS на средства АУЦ? Сможете провести?
Оценка влияния занимает от 1 года до 1.5 лет. При необходимости проведем.

60. Подскажите в каких случаях в hsm на контейнер ставится pin-код 8 единиц?
Уточните, пожалуйста, вопрос.

61. При создании ключа ЭП при визите в АУЦ, допустимо ли изготавливать ключ ЭП не самим пользователем?
Да, допустимо.

62. При использовании облачной ЭП для ЮЛ и при входе в ЛК ЮЛ ФНС приходится подтверждать порядка 20 раз обращение к ЗК в приложении myDSS, хотя при работе облачной ЭП ФЛ такой проблемы не происходит. проходили ли подобного рода тесты с Вашей стороны? как выйти из данной ситуации?
Со стороны ЛК ЮЛ ФНС необходимо уменьшить количество обращений к ЗК

63. Зачем NGate в DSS? Он заменяет сервер аутентификации из состава DSS?
NGate здесь опционален. Он может повысить защищённость подключения к DSS и снять часть нагрузки по TLS с сервера DSS.

64. Планируется ли более упрощённая настройка в DSS’е ? Например, через Веб-интерфейс?
Планируется реализовать толстый клиент.

65. Есть ли возможность протестировать myDSS на Вашем тестовом сервисе? Есть инструкция по настройке?
Да, ссылки доступны на слайде.

66. Планируете в DSS реализовать поддержку CAdES-A? Если да, то когда?
Планируется, на данный момент точных сроков нет.

67. Есть ли возможность или планируется реализовать функционал (через Веб-интерфейс или по API) – в усовершенствованной подписи удалить имеющиеся доказательства подписи и на выходе получить CAdES BES?
Планируется.