Вопросы и ответы с вебинара «Эволюция электронной подписи в смартфоне. Варианты реализации в соответствии с законодательством» от 25.11.20 г.

1. **Принимают ли участие специалисты КРИПТО-ПРО в подготовке приказа ФСБ России о требованиях к дистанционной "облачной" подписи?** В подготовке - нет. Принимаем участия в консультациях при подготовке приказа Службой.
2. **Как Вы думаете, до конца года проект приказа будет размещен для общественного обсуждения?** Надеемся, но зависит не от нас.
3. **Требуются ли на Ваш взгляд какие изменения в 63-ФЗ в части использования мобильной подписи?** Нет, не требуются.
4. **Требуется ли проведение оценки влияния при интеграции myDSS в стороннее приложение?** По нашему мнению, для "Госов" - требуется, для остальных – нет.
5. **На сколько экономически выгодно использовать DSS?** Если вы хотите поставить инхаус, то инхаус поставка становится выгодна от 10 000 пользователей. Но сейчас почти все УЦ предоставляют возможность использования их инфраструктуры для работы с myDSS, закладывая стоимость использования в стоимость сертификата (будь то КЭП или НЭП). И стоимость такого внешнего использования очень невелика. Таким образом можно в любом случае подобрать выгодный вариант. Обращайтесь - поможем с выбором варианта поставки или УЦ.
6. **В ЖТЯИ указано, что для назначения устройства с помощью alias необходимо получить ручную подпись клиента в заявительных документах. Планируется ли добавить опции по назначению устройства (например, допустить подписание ПЭП/ПЭП ЕСИА вместо ручной подписи заявителя).** Назначение устройства - критическая с точки зрения безопасности функция. На безопасном выполнении этой привязки основывается безопасность использования схемы целиком, поэтому механизм подтверждения alias должен быть надёжным. Поэтому ПЭП с неизвестными (читай, недоказанными) свойствами защищённости не подходит.
7. **В августе 2021 годи истекли сроки действия сертификатов соответствия на DSS, продление не планируется, что делать тем, кто ранее купил и использует DSS?** Продление планируется (вернее, новая сертификация), но это возможно уже только при сертификации по требованиям к средствам дистанционной подписи. Сейчас для КЭП можно использовать мобильную подпись (с хранением ключей ЭП на смартфоне).
8. **Сами ключи ЭП точно хранятся в самом HSM?** Вроде как раньше хранились в базе DSS в зашифрованном виде. Можно и так, и так. Безопасность зашифрованных и хранящихся в базе данных ключей при этом всё равно обеспечивается ключом, хранимым в HSM.
9. **Как производится дополнение подписи до усовершенствованной?** Добавляются необходимые доказательства подлинности - метки времени, сертификаты, OCSP-ответы.
10. **"Мобильный" ключ является экспортируемым? Возможен ли перенос ключей с "мобильного" токена в случае смены телефона.** Сейчас не возможен, для будущих версий прорабатываем безопасный способ переноса.
11. **С 2022 для руководителей ЮЛ и ИП выпускаться должны подписи ТОЛЬКО в ФНС. ФНС выпускать DSS подписи не будет и не планирует. Т.е. DSS доступна будет только для сотрудников. С ИП проблем еще больше. Как это коррелируется с Вашим утверждением об использовании DSS для МСБ?** Планы ФНС на данный момент имеют несколько вариантов развития. Однако уже сейчас есть концепция доверенных УЦ, которые могут выпускать КЭП на myDSS.
12. **Я правильно понял, что myDSS позволяет использовать сертификаты и формировать ЭП, как неквалифицированную, так квалифицированную?** Да.

13. **Чем концептуально (принципиально) отличается Ваше мобильное приложение от приложения "Госключ"?** Если совсем принципиально - приложение может работать как с дистанционной подписью (ключ ЭП хранится в HSM), так и с мобильной (ключ ЭП хранится в смартфоне).
14. **Как обеспечивается безопасность приложения на смартфонах (взломы, атаки)?** Используется комбинация встроенных в современные мобильные ОС средств защиты и средства защиты, встроенные КриптоПро CSP.
15. **Допустимо ли использование вашего решения при отсутствии требований ФСБ к дистанционной "облачной" подписи и как следствие в отсутствии аккредитации по дополнительным требованиям к хранению ключей?** Да, в режиме мобильной подписи.
16. **Сколько стоит технология для конечного клиента?** Если вы хотите поставить инхаус - направьте нам запрос на расчет, т.к. очень много параметров при формировании стоимости. Если хотите использовать инфраструктуру УЦ, то обратитесь в УЦ, вам сообщат стоимость вместе с сертификатом (будь то НЭП или КЭП). В среднем использование именно myDSS (без учета сертификатов) варьируется от 200 рублей в год.
17. **Существует ли требование регулятора, которое обязывает использование технологии myDSS?** Регулятор предъявляет требования к тому, чтобы средство ЭП было сертифицировано. Выбор же соответствующего средства остается за владельцем системы или пользователем.
18. **Если ключ в смартфоне, то как ведется учет СКЗИ и чья это зона ответственности?** Сами пользователи учет не ведут. Владелец сервиса может учитывать СКЗИ пользователей подключая их к сервису и выдавая им сертификаты.
19. **Хотелось бы узнать о рисках использования технологии myDSS в части ИБ.** Тут трудно коротко ответить. Если совсем коротко - всё описано в документации на средства подписи. Если подробнее, то лучше лично пообщаться.
20. **А почему вы не акцентируете внимание на том, что по требованию заказчика (настоящее рекомендация регулятора) тоже необходимо проводить оценку влияния?** Все верно, если заказчику это необходимо, то оценка влияния по его желанию может быть проведена.
21. **Есть ли возможность работы пользователю со своим персональным сертификатом через DSS с разными системами в рамках одного логина или для каждой системы надо заводить свой логин и свои сертификаты?** Да, в разных системах разные учетные записи. Но в будущем планируем сделать обобщающий хаб.
22. **Планируется ли реализация применения ЭП на гос.ресурсах?** Этот вопрос лежит в ведении владельца ресурса, мы как производитель предоставляем только продукт, который эту задачу может решить уже сейчас.
23. **Для использования "мобильной" подписи необходимо обновить дистрибутив до ПАК «КриптоПро DSS» версии 2.0 (сборка 3714), верно? При этом, последняя сертифицированная версия - это ПАК "КриптоПро DSS" версии 2.0 (сборка 2.0.3284). Получается решение для квалифицированных сертификатов все равно не легитимно, пока ПАК 3714 не сертифицируют?** Для использования в режиме мобильной подписи DSS не играет роль СКЗИ.
24. **А другие программы готовы к такому взаимодействию? Сейчас есть какая-то информация, какие сервисы поддерживают myDSS 2.0?** Часть УЦ можно увидеть в приложении myDSS 2.0.
25. **Все ли документы визуализируются? Формы для визуализайции вы сами разрабатывали?** Документы визуализируются с помощью плагинов встроенных в сервер DSS. Для большинства форматов есть встроенные плагины, но вы можете написать свои для своих форматов.

26. **Какой процесс выдачи “мобильной подписи” планируется? От момента возникновения потребности до момента начала пользования?** Показывали на демонстрации - примерно такой же процесс, только вместо демостранички - личный кабинет УЦ
27. **Будет ли реализована (документированная) работа мобильного приложения myDSS через deeplink для использования в мобильном броузере (с передачей данных в обе стороны или гарантированным возвратом в браузер)?** В планах.
28. **Будет ли поддержка токенов (NFC, BT) в DSS SDK?** Будет.
29. **Можно ли получить тестовую версию myDSS 2.0, посмотреть возможности кастомизации?** Да, вы можете использовать наш тестовый сервер. Напишите нам на info@cryptopro.ru.
30. **Правильно ли поняла, что Мобильную электронную подпись (с хранением ключа ЭП на смартфоне) можно уже сейчас использовать для квалифицированной подписи и технология имеет все нужные сертификаты?** Да, всё именно так.
31. **Как обеспечивается резервная копия мобильного ключа ЭП?** Реализация данного функционала в планах.
32. **Какой статус разработки DSS и ПАК КриптоПро УЦ для Linux?** Когда можно будет попробовать, протестировать? Ориентировочно вторая половина 2022 года
33. **Новая сертификация DSS+УЦ позволит понизить уровень нарушителя и подключить УЦ к сети Интернет?** Это будет зависеть от требований ФСБ, которых пока нет.
34. **После установки приложения и выпуска сертификата, пользователь может удалить приложение. Существует ли возможность с бэка проверить активность приложения (установлено ли оно все еще)? Если нет, планируется ли реализовать возможность такой проверки?** Да, при удалении приложения ключи тоже будут удалены. Проверка активности приложения технически невозможна. Можно периодически отправлять документы на подпись.
35. **Можно ли мобильную ЭП перенести на другое устройство в случае утери или удаления с мобильного телефона? Можно ли приостановить действие сертификата либо отозвать его через приложение?** Сейчас перенести нельзя. Приостановление действия сертификата и его отзыв в планах.
36. **С 2021 для руководителей ЮЛ и ИП подписи (сертификаты) должны выпускаться ТОЛЬКО в ФНС. ФНС выпускать DSS подписи не будет и не планирует. Т.е. DSS будет доступен только для сотрудников. С ИП проблем еще больше. Как это коррелируется с Вашим утверждением об использовании DSS для МСБ?** Доверенные лица УЦ ФНС используют разные технологии. А филиалы доверенных лиц еще более разные технологии. Вопрос только в аккредитации (и в наличии сертификата регулятора). Так что фундаментальных противоречий нет.
37. **Какой планируется workaround если у части сотрудников предприятия (на котором внедрена ЭП для кадрового документооборота) нет смартфона IOS или Android?** Варианты есть, напишите нам на info@cryptopro.ru и мы расскажем как.
38. **Что делать с имеющимися у нас DSS и ПАК УЦ после сертификации обоих "в одном флаконе"?** Необходимо обновить версию DSS и УЦ и использовать их в необходимом режиме – дистанционной («облачной») или мобильной подписи (ключ хранится в смартфоне).
39. **Есть ли API для автоматического создания профиля?** Да. Через API можно сделать почти все. Но некоторые вещи, которые нужно подтверждать на смартфоне, обойти нельзя по требованиям сертификации.
40. **Могу ли я получить несколько КЭП в разных УЦ? И как это будет выглядеть в моем мобильном приложении myDSS 2.0? У меня при этом будет несколько разных учетных записей DSS?** Можете. У вас будет несколько профилей в приложении и несколько учетных записей в DSS.

41. **С какими решениями других компаний совместимы подписи для документов MS Office, PDF, XML?** Используются только стандартные форматы подписи.
42. **Можно ли один сертификат одновременно хранить на нескольких устройствах и работать с ним?** При системе хранения ключей на смартфоне технически это невозможно. А при хранении на HSM – да, это возможно.
43. **С какими УЦ вы уже совместно работаете и что нужно, чтобы "подключить" новый УЦ?** Список УЦ достаточно большой, обратитесь пожалуйста на info@cryptopro.ru
44. **Как будет выглядеть процедура получения сертификата в аккредитованном УЦ? Пользователь должен идентифицироваться и ознакомиться с содержимым сертификата?** В аккредитованном УЦ все должно быть по закону. Но каких-то ограничений со стороны системы для реализации требований законодательства нет.
45. **Мобильный телефон - это недоверенная среда. Как осуществляется защита закрытого ключа?**
46. **Все-таки, myDSS 2.0 - он для среднего и малого бизнеса или же применим также и для крупного со своей облачной инфраструктурой подписания?** Крупный бизнес для внутреннего использования и внутреннего ЭДО. МСБ для внешнего (онлайн-бехгалтерии, Банки и пр.)
47. **В дополнение по вопросу назначения устройства и подписания заявительных документов с указанием alias - ПЭП ЕСИА также является недостаточно надежным способом?** ПЭП ЕСИА не проходила оценку безопасности со стороны ФСБ России, поэтому не является надежным способом.
48. **Можно ли из приложения myDSS отправить подписанный документ кому-либо, нажав кнопку "поделиться"?** Да, это будет доступно уже в ближайшем релизе.
49. Есть, ли у вас примеры легитимной архитектуры подписания с использованием ИС инициатора подписания (интеграция через API), КриптоПро DSS и myDSS, которая соответствует требованиям ФЗ-63? Да. Можете обратиться к нам за консультацией на info@cryptopro.ru.
50. **Можно ли импортировать существующий сертификат так, чтобы ключ хранился в мобильном приложении, а не на сервере?** Пока поддерживаются только ключи, созданные внутри приложения.
51. **Реализовано ли пакетное подписание? Можно ли отправить одновременно два и более документов на подписание?** Да.
52. **Крупному бизнесу интересны пакетные подписания документов. Какие возможности предоставляет связка КриптоПРо DSS и MyDSS2.0?** Режим подписания пакета документов за одну операцию в мобильном телефоне как раз реализован в myDSS 2.0
53. **При удалении или сбросе устройства на заводские настройки мы попрощаемся с сертификатом, который хранился на устройстве?** Функционал бэкапирования в планах. Пока он не реализован ключ будет удалён без возможности восстановления.
54. **В myDSS 2.0 постоянно высвечивается информация о желательности использования антивирусного ПО.** Какие риски клиенты будут иметь, если антивирусное ПО не будет использоваться? Наличие антивируса на Android - требование сертификации.
55. **Для прозрачной работы с мобильной подписью потребуется, как и прежде, установка CloudCSP?** Связка с Cloud CSP также работает и с мобильным режимом хранения ключей, как ранее работала с облачной. Тут ничего не поменялось.
56. **При пакетном подписание есть отображение документов в мобильном приложении?** Да, есть
57. **Есть ли какие-то лицензионные или юридические риски, если myDSS2.0 будет устанавливаться на личные устройства пользователей, а владельцем лицензии будет являться юридическое лицо?** Лицензию на использование приобретает юр.лицо – владелец DSS. А мобильное приложение

распространяется бесплатно из магазина приложений и каких-то юридических рисков мы тут не видим.

58. **Какие версии мобильных ОС допустимы к использованию и что делать при их обновлении?** Информацию по версиям см. в формуляре на КриптоПро CSP 5.0 R2. При обновлении ОС мы как производитель проводим процедуру новой сертификации.
59. **Alias можно указывать в заявлении на выпуск КЭП? Какая формулировка должна быть в заявительных документах для назначения устройства с использованием alias?** Сертификат на КриптоПро CSP довольно «длинный» и нет необходимости об этом беспокоиться.
60. **Требуется ли доверенный канал между мобильным приложением и сервисом DSS при выпуске сертификата?** Канал между смартфоном и DSS зашифрован по ГОСТу.
61. **Где можно посмотреть требования SDK myDSS 2.0 к ОС Android и IOS, требования к железу?** Обратитесь, пожалуйста, на info@cryptopro.ru.
62. **Был вопрос "Допустимо ли использование использовать Ваше решение при отсутствии требований ФСБ к дистанционной "облачной" подписи?" при ответе на который было сказано, что можно использовать только в режиме мобильной подписи. Правильно ли я понимаю, что по сути технология DSS до сих пор не сертифицирована ФСБ и использование ее нелегитимно? Как тогда УЦ ее используют и предоставляют на коммерческой основе другим?** За все УЦ ответить не готовы, а те УЦ, с которыми мы работаем в настоящее время, переходят на использование режима мобильной подписи (хранение ключа ЭП в смартфоне).
63. **В каком СКЗИ HSM (не сертифицированном) или CSP 5.0 R2 (сертифицированном) осуществляется вычисление ХЭШ-значений при использовании мобильной подписи? Если HSM, то допустимо ли ХЭШ для УКЭП вычислять несертифицированным средством ЭП?** Сам HSM – сертифицирован. Истекли только сертификаты на исполнение HSM с DSS, но для использования myDSS в режиме мобильной подписи (хранение ключа ЭП на смартфоне) сертификат на DSS не требуется. ХЭШ-значение вычисляется в смартфоне, т.е. используется КриптоПро CSP 5.0 R2.
64. Как будет реализована процедура получения сертификата в аккредитованном УЦ (идентификация, ознакомление с содержимым сертификата)? Напишите нам на info@cryptopro.ru, покажем.
65. Разве КЭП не должна храниться на защищенном сертифицированном носителе? Каждый телефон не сертифицируешь. Отдельных требований по сертификации ключевых носителей – нет.
66. **Какая(ие) СУБД будет использоваться в ПАК КриптоПро DSS под Linux?** PostgreSQL
67. **Может ли сим-карта смартфона использоваться как аппаратный криптопровайдер и хранилище ключа? Есть ли такая возможность в myDSS? Если нет, будет ли?** С нашей стороны соответствующие доработки есть, использование с myDSS технически возможно, ждем появления соответствующей сертифицированной сим-карты.
68. **Каким образом обеспечена защита персональных данных (ПДн) при регистрации и использовании? Разрешение на использование ПДн не запрашивается при регистрации?** Передача данных между компонентами решения осуществляется по защищенному по ГОСТ каналу. Остальные вопросы защиты лежат на стороне владельца системы.
69. **Должен ли я хранить телефон с записанной на нем ключевой информацией в сейфе?** Конечно же нет, просто держите смартфон при себе и в безопасности.
70. **Про мобильное устройство - как защищенное хранилище ключа: Формуляр КриптоПро CSP 5/0 обязывает устанавливать совместно с СКЗИ антивирус, сертифицированный в ФСБ. Прокомментируете, пожалуйста.** Для IOS установка антивируса не требуется (согласно формуляру). Для Андроид установка необходима, соответствующие антивирусы есть в магазине приложений.