Дистанционное создание электронной подписи: настоящее и будущее

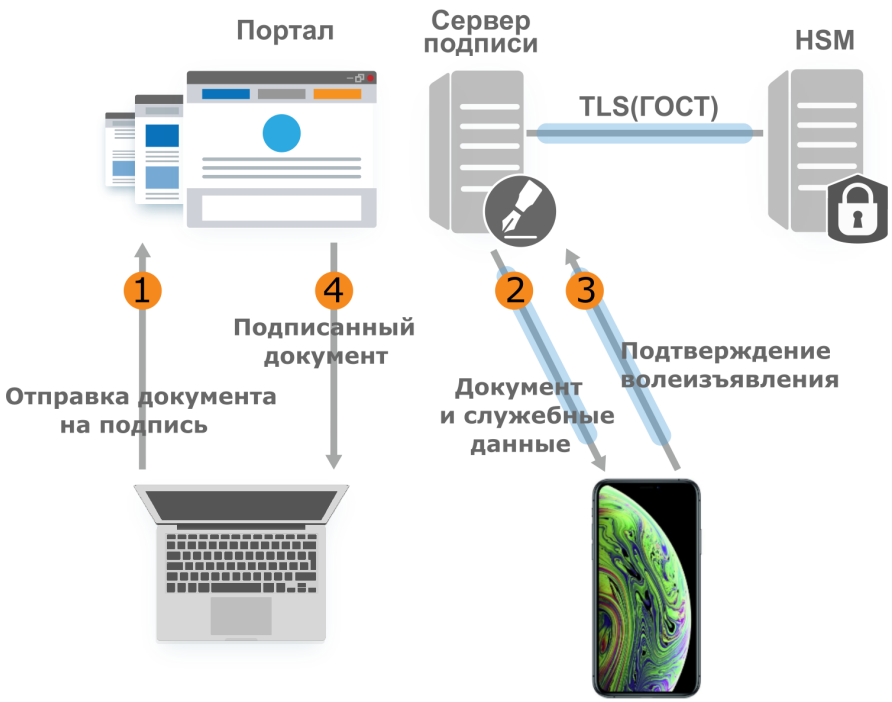
Смышляев Станислав Витальевич, к.ф.-м.н.,
заместитель генерального директора
Смирнов Павел Владимирович, к.т.н.,
директор по развитию

Изменения “ландшафта” рынка электронной подписи

- 476-ФЗ, подзаконные НПА.
- Информационная безопасность: уточненные модели угроз, отдельные группы требований для классов средств.
- Как и всегда, рынку нужны одновременно удобные и безопасные решения.

Дистанционное формирование подписи

Дистанционное формирование подписи



- Единое решение: серверная и клиентская компоненты.
- Серверная компонента — защищенное хранение ключей в неизвлекаемом виде, реализация операций по аутентифицированным запросам от клиентских компонент.
- Клиентская компонента — визуализация, аутентификация, волеизъявление на совершение операций, защищенный канал.

Преимущества

- Пользователь имеет возможность доступа к своим ключам ЭП с нескольких устройств, что удобно для «мобильных» сотрудников и для руководителей высшего звена.
- Высокопроизводительные кластеризуемые аппаратные решения на стороне сервера — высокая скорость подписания пакетов документов.
- Возможность прямого взаимодействия серверных компонент средства подписи с ИС позволяет по желанию владельца ключа ограничить допустимое множество документов, поступающих ему на подпись.
- Возможность бесшовного перехода любых ранее написанных прикладных систем.

Преимущества

- Средство аутентификации налагает существенно меньшее количество требований к окружению, чем средство ЭП, что позволяет упростить порядок установки и распространения, расширить перечень устройств.
- Риски компрометации ключа ЭП при сбоях ДСЧ отсутствуют.
- Максимально подробный аудит на серверной стороне с защитой журналов в HSM класса КВ с помощью цепной записи данных.
- Возможность для конкретных видов данных определять оптимизированные сценарии просмотра и подтверждения операций.
- Повреждение/утеря устройства аутентификации не приводит к утере ключей ЭП, в случае утери доступ к ключам блокируется мгновенно на серверной стороне.

Обеспечение информационной безопасности

Подтверждённая сертификатом безопасность — реальное использование решения осуществляется ровно так, как предполагает согласованная с ФСБ России документация.

- Проблема обновления версий.
- Скачивание мобильных приложений.
- Обеспечение безопасности окружения.
- Безопасность ДСЧ.
- Работа только по каналу с TLS-ГОСТ.
- Честная и удобная визуализация документов.
- Возможность удобно и безопасно проводить идентификацию пользователя в момент, когда у него появляется ключ.
- Реальная интеграция с существующим прикладным ПО в соответствии с документацией на сертифицированное средство.

Интеграция с существующими приложениями

Пример “адаптеров” для ЕБС

Задача обеспечить возможность интеграции со сторонним прикладным ПО — в некотором смысле аналогична той, что решалась при создании типовых решений для банков для подключения с ЕБС.

Интерфейс для встраивания в существующие приложения

Принципы решения для интеграции в существующие приложения:

- Самодостаточность процесса
- Обработка всех ошибок и нештатных ситуаций в рамках встраиваемых модулей.
- “Защита от дурака”

Порядок идентификации владельца

- Доклад “Подходы к удаленной идентификации и аутентификации для задач PKI: как совместить цифровую экономику и безопасность” на PKI-Форум Россия 2018.
- Принцип:
  1. создать неподтвержденную учетную запись, обеспечив пользователя ключами и средствами аутентификации/волеизъявления для работы с ней;
  2. создать ключи ЭП в рамках этой учетной записи, а также запросы на сертификаты;
  3. тем или иным легитимным способом подтвердить личность пользователя для выпуска сертификата и привязки учетной записи к нему как к физическому/юридическому лицу.
- Схема в полной мере реализована в обновленных исполнениях КриптоПро DSS.

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер **СФ/124-3881** от "**07**" **августа** 2020 г.

Действителен до "**01**" **февраля** 2023 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что изделие **«Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0 (комплектация 1)** (исполнения: 1, 2, 3, 4, 5) в комплектации согласно формуляру ЖТЙИ.00096-01 30 01 с учётом изменений согласно извещению ЖТЙИ.00096-01-2019

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнения 1), класса КС3 (для исполнений: 2, 3, 4, 5). Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1 (для исполнения 1), класса КС2 (для исполнения 2), класса КС3 (для исполнений: 3), и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, криптографическая аутентификация абонентов при установлении соединения, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «КРИПТО-ПРО»

сертификационных испытаний образца продукции № 789А-011001

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ЖТЙИ.00096-01 30 01 с учётом изменений согласно извещению ЖТЙИ.00096-01-2019.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **О.В. Скрябин**

Настоящий сертификат внесён в Государственный реестр сертификатов средств защиты информации 7 августа 2020 г.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России Д.А. Кругов

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер **СФ/124-3882** от "**07**" **августа** 2020 г.

Действителен до "**01**" **февраля** 2023 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что изделие **«Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0 (комплектация 2)** (исполнения: 1, 2, 3) в комплектации согласно формуляру ЖТЙИ.00096-01 30 01 с учётом изменений согласно извещению ЖТЙИ.00096-01-2019

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнения 1), класса КС2 (для исполнения 2), класса КС3 (для исполнения 3). Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1 (для исполнения 1), класса КС2 (для исполнения 2), класса КС3 (для исполнений: 3), и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, криптографическая аутентификация абонентов при установлении соединения, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «КРИПТО-ПРО»

сертификационных испытаний образца продукции № 789А-011001

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ЖТЙИ.00096-01 30 01 с учётом изменений согласно извещению ЖТЙИ.00096-01-2019.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **О.В. Скрябин**

Настоящий сертификат внесён в Государственный реестр сертификатов средств защиты информации 7 августа 2020 г.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России Д.А. Кругов

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер **СФ/124-3883** от "**07**" **августа** 2020 г.

Действителен до "**07**" **августа** 2021 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что изделие **«Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0 (комплектация 3)** (исполнение: «DSS + CSP» версия 4.0 Исполнение 1-Base», «DSS + CSP» версия 4.0 Исполнение 2-Base», «DSS + CSP» версия 4.0 Исполнение 3-Base») в комплектации согласно формуляру ЖТЙИ.00096-02 30 01 с учётом изменений согласно извещению ЖТЙИ.00096-02-2019

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнения «DSS + CSP» версия 4.0 Исполнение 1-Base»), класса КС2 (для исполнения «DSS + CSP версия 4.0 Исполнение 2-Base»), класса КС3 (для исполнения «DSS + CSP» версия 4.0 Исполнение 3-Base»). Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1 (для исполнения «DSS + CSP версия 4.0 Исполнение 1-Base»), класса КС2 (для исполнения «DSS + CSP версия 4.0 Исполнение 2-Base»), класса КС3 (для исполнения «DSS + CSP» версия 4.0 Исполнение 3-Base»), и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, криптографическая аутентификация абонентов при установлении соединения, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «КРИПТО-ПРО»

сертификационных испытаний образца продукции № 789А-011002

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ЖТЙИ.00096-02 30 01 с учётом изменений согласно извещению ЖТЙИ.00096-02-2019.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **О.В. Скрябин**

Настоящий сертификат внесён в Государственный реестр сертификатов средств защиты информации 7 августа 2020 г.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России Д.А. Кругов

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер **СФ/124-3884** от "**07**" **августа** 2020 г.

Действителен до "**07**" **августа** 2021 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что изделие **«Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0 (комплектация 2а)** в комплектации согласно формуляру ЖТЙИ.00096-02 30 01 с учётом изменений согласно извещению ЖТЙИ.00096-02-2019

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1, Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1, и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, криптографическая аутентификация абонентов при установлении соединения, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «КРИПТО-ПРО»

сертификационных испытаний образца продукции № 789А-011002

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ЖТЙИ.00096-02 30 01 с учётом изменений согласно извещению ЖТЙИ.00096-02-2019.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **О.В. Скрябин**

Настоящий сертификат внесён в Государственный реестр сертификатов средств защиты информации 7 августа 2020 г.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России Д.А. Кругов

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер **СФ/124-3885** от "**07**" **августа** 2020 г.

Действителен до "**07**" **августа** 2021 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что изделие **«Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0 (комплектация 3)** (исполнение: «DSS + SIM (OES)», «DSS + SIM (M2M)») в комплектации согласно формуляру ЖТЙИ.00096-02 30 01 с учётом изменений согласно извещению ЖТЙИ.00096-02-2019

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1. Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1, и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, криптографическая аутентификация абонентов при установлении соединения, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «КРИПТО-ПРО»

сертификационных испытаний образца продукции № 789А-011002

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ЖТЙИ.00096-02 30 01 с учётом изменений согласно извещению ЖТЙИ.00096-02-2019.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **О.В. Скрябин**

Настоящий сертификат внесён в Государственный реестр сертификатов средств защиты информации 7 августа 2020 г.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России Д.А. Кругов

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер **СФ/124-3886** от "**07**" **августа** 2020 г.

Действителен до "**07**" **августа** 2021 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что изделие **«Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0 (комплектация 3)** (исполнение: «DSS + mySDSS», «DSS + AirKey Lite») в комплектации согласно формуляру ЖТЙИ.00096-02 30 01 с учётом изменений согласно извещению ЖТЙИ.00096-02-2019

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1. Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1, и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, криптографическая аутентификация абонентов при установлении соединения, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «КРИПТО-ПРО»

сертификационных испытаний образца продукции № 789А-011002

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ЖТЙИ.00096-02 30 01 с учётом изменений согласно извещению ЖТЙИ.00096-02-2019.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **О.В. Скрябин**

Настоящий сертификат внесён в Государственный реестр сертификатов средств защиты информации 7 августа 2020 г.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России Д.А. Кругов

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер **СФ/124-3887** от "**07**" **августа** 2020 г.

Действителен до "**07**" **августа** 2021 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что изделие **«Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0 (комплектация 3)** (исполнение: «DSS + CSP» версия 4.0 Исполнение 1-Lic», «DSS + CSP» версия 4.0 Исполнение 2-Lic») в комплектации согласно формуляру ЖТЙИ.00096-02 30 01 с учётом изменений согласно извещению ЖТЙИ.00096-02-2019

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнения «DSS + CSP» версия 4.0 Исполнение 1-Lic»), класса КС2 (для исполнения «DSS + CSP версия 4.0 Исполнение 2-Lic»). Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1 (для исполнения «DSS + CSP версия 4.0 Исполнение 1-Lic»), класса КС2 (для исполнения «DSS + CSP» версия 4.0 Исполнение 2-Lic»), и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, криптографическая аутентификация абонентов при установлении соединения, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «КРИПТО-ПРО»

сертификационных испытаний образца продукции № 789А-011002

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ЖТЙИ.00096-02 30 01 с учётом изменений согласно извещению ЖТЙИ.00096-02-2019.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **О.В. Скрябин**

Настоящий сертификат внесён в Государственный реестр сертификатов средств защиты информации 7 августа 2020 г.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России Д.А. Кругов

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер **СФ/124-3888** от "**07**" **августа** 2020 г.

Действителен до "**07**" **августа** 2021 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что изделие **«Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0 (комплектация 3)** (исполнение: «DSS + CSP версия 5.0 КС1 Исполнение 1-Base», «DSS + CSP версия 5.0 КС2 Исполнение 2-Base», «DSS + CSP версия 5.0 КС3 Исполнение 3-Base») в комплектации согласно формуляру ЖТЙИ.00096-02 30 01 с учётом изменений согласно извещению ЖТЙИ.00096-02-2019

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнения «DSS + CSP версия 5.0 КС1 Исполнение 1-Base») класса КС2 (для исполнения «DSS + CSP версия 5.0 КС2 Исполнение 2-Base»), класса КС3 (для исполнения «DSS + CSP версия 5.0 КС3 Исполнение 3-Base»). Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1 (для исполнения «DSS + CSP версия 5.0 КС1 Исполнение 1-Base»), класса КС2 (для исполнения «DSS + CSP версия 5.0 КС2 Исполнение 2-Base»), класса КС3 (для исполнения «DSS + CSP версия 5.0 КС3 Исполнение 3-Base») и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, криптографическая аутентификация абонентов при установлении соединения, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «КРИПТО-ПРО»

сертификационных испытаний образца продукции № 789А-011002

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ЖТЙИ.00096-02 30 01 с учётом изменений согласно извещению ЖТЙИ.00096-02-2019.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **О.В. Скрябин**

Настоящий сертификат внесён в Государственный реестр сертификатов средств защиты информации 7 августа 2020 г.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России Д.А. Кругов

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер **СФ/124-3889** от "**07**" **августа** 2020 г.

Действителен до "**07**" **августа** 2021 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что изделие **«Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0 (комплектация 3)** (исполнение: «myDSS SDK», «Сбербанк mDSS SDK», «DSS Client SDK») в комплектации согласно формуляру ЖТЙИ.00096-02 30 01 с учётом изменений согласно извещению ЖТЙИ.00096-02-2019

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1. Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1, и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, криптографическая аутентификация абонентов при установлении соединения, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «КРИПТО-ПРО»

сертификационных испытаний образца продукции № 789А-011002

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ЖТЙИ.00096-02 30 01 с учётом изменений согласно извещению ЖТЙИ.00096-02-2019.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **О.В. Скрябин**

Настоящий сертификат внесён в Государственный реестр сертификатов средств защиты информации 7 августа 2020 г.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России Д.А. Кругов

Ожидаемые требования к средствам ОКЭП

476-ФЗ: отдельные уточненные требования для средств дистанционного формирования электронной подписи

- Новые уточненные требования, учитывающие особенности систем, нужны.
- Их отсутствие не должно приводить к использованию средств, не удовлетворяющих общим требованиям к СКЗИ/СЭП.
- Основные принципы и фундамент всегда один: безопасность должна базироваться на доказуемо стойких решениях, с проведением исследований и получением заключения ФСБ.
- Уточнения полезны. Принципы в сертифицированных решениях выполняются.

Ожидаемые требования к средствам ОКЭП

Принципы соответствия 4 группам требований

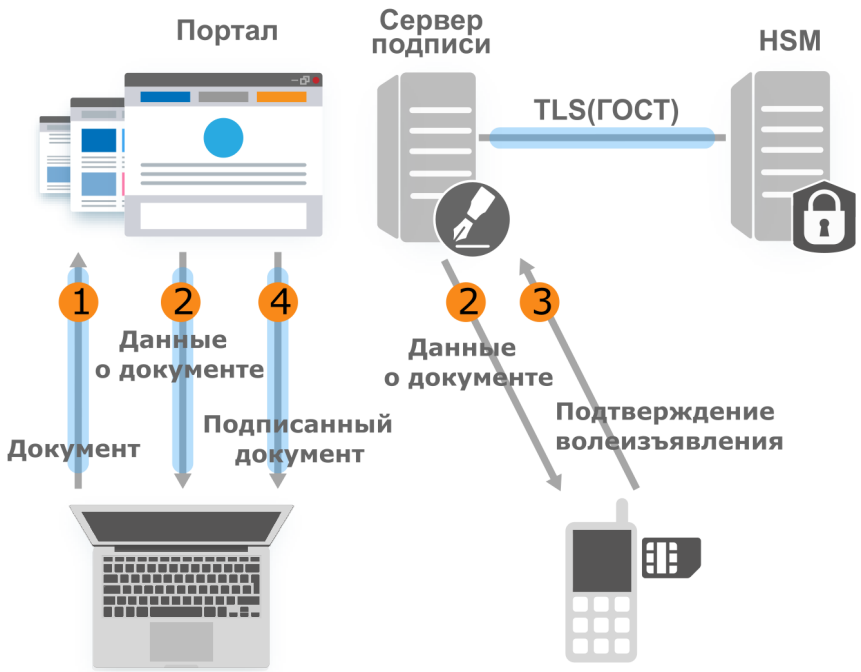
1. Создание, хранение, использование, уничтожение ключей: с использованием ПАКМ “КриптоПро HSM” 2.0 (класс КВ2), хранение ключей в неизвлекаемом виде в продолжение всего их жизненного цикла.
2. Аутентификация владельцев сертификатов для каждой транзакции с помощью полноценных 256-битовых ключей.
3. Защита всей информации с помощью TLS с ГОСТ.
4. Доверенное отображение документов, однозначность отображения результатов операций, аутентифицированное подтверждение операций (с привязкой отображенной информации), доверенный аудит всех операций с ключами ЭП в HSM на основе использования механизмов цепной записи данных.

Ближайшее будущее

Направления развития КриптоПро DSS

- Досертификация по отдельным требованиям к средствам дистанционного формирования электронной подписи.
- Поддержка перспективных доверенных SIM-карт (класс КС3).
- Удаленное получение сертификата без личной явки.

Поддержка защищенных SIM-карт



Получение сертификатов без личной явки

Еще одна норма 476-ФЗ

К традиционным способам идентификации заявителя при выдаче сертификата ключа проверки электронной подписи добавляются дистанционные, посредством идентификации заявителя без его личного присутствия путем предоставления сведений из ЕСИА и ЕБС, а также с помощью заграничного паспорта нового поколения.

Реализация таких возможностей требует проработки технических и криптографических вопросов.

Удаленное получение сертификата без личной явки

Готовность КриптоПро DSS к удаленному получению сертификатов

1. Пользователь по защищенному каналу с односторонней аутентификацией обращается к серверу подписи, запрашивает генерацию нового ключа с получением аутентификатора к нему, а также запроса на сертификат.
2. Пользователь обращается в УЦ, аутентифицируется и авторизуется с помощью ЕСИА+ЕБС или ЕСИА+загранпаспорта, после чего пересылает по созданному защищенному каналу запрос на сертификат в УЦ.
3. УЦ выпускает квалифицированный сертификат на данного пользователя, передает его пользователю.
4. Пользователь пересылает полученный сертификат на сервер.
5. Пользователь использует свой ключ в средстве ЭП обычным образом с помощью аутентификатора.

CRYPTOPRO

Спасибо за внимание!

Вопросы?

- Материалы, вопросы, комментарии:
  svs@cryptopro.ru
  spv@cryptopro.ru