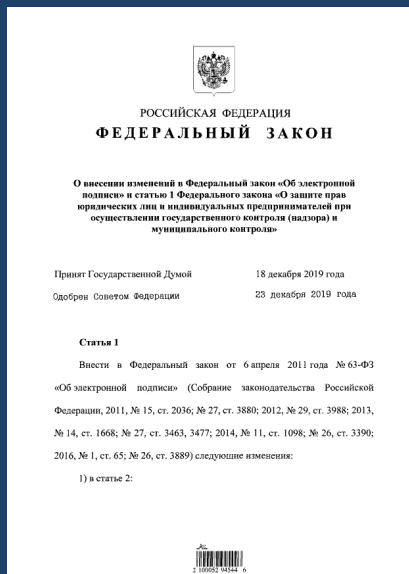


Использование средств ЭП класса КВ2 доверенными лицами УЦ ФНС России: взгляд вендора на реализацию требований 171 приказа

Бадмаева Римма
Ведущий менеджер продуктов





ФЗ от 27.12.2019 №476-ФЗ
«О внесении изменений в
Федеральный закон «Об
электронной подписи»

Предпосылки

Статья 15 дополнена частью 6.1 о наделении доверенных лиц (ДЛ) полномочиями на прием заявлений о получении квалифицированного сертификата ЮЛ, создание ключа ЭП и т.п. ДЛ должны, в том числе, соответствовать организационно-техническим требованиям в области ИБ, установленным ФСБ России.

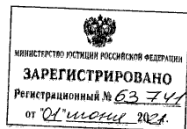


ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

1 мая 2021 года Москва № 171

Об утверждении организационно-технических требований в области информационной безопасности к доверенным лицам удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц



В соответствии с частью 6.1 статьи 15 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»¹ и пунктом 1 Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 г. № 960²,

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемые организационно-технические требования в области информационной безопасности к доверенным лицам удостоверяющего центра федерального органа исполнительной власти,

¹ Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; 2019, № 52, ст. 7794.

² Собрание законодательства Российской Федерации, 2003, № 33, ст. 3254; 2007, № 1, ст. 205.

Предпосылки

Приказ ФСБ России от 01.05.2021 №171 «Об утверждении организационно-технических требований в области информационной безопасности к доверенным лицам удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц»

Приказ ФСБ России №171

В пункте 8 было определено, что при создании ключа ЭП по обращению заявителей ДЛ должно:

- применять **средства ЭП KB2** или КА1, имеющие в своем составе датчик, вырабатывающий случайную последовательность и механизм контроля срока действия ключей ЭП;
- записывать ключи ЭП, созданные по обращению заявителя, **на специализированные ключевые носители**, исключающие их несанкционированное использование и копирование;
- хранить, использовать и уничтожать ключи ЭП доверенного лица, предназначенные для подписания электронных документов и информации, в средстве ЭП, в котором они были созданы;
- применять СКЗИ, не являющиеся средствами ЭП, классов KB и (или) КА;
- применять средства ЭП классов, отличных от классов KB2 и (или) КА1, СКЗИ, не являющиеся средствами ЭП, классов, отличных от классов KB и (или) КА, в схеме доставки заявления о получении квалифицированного сертификата юридического лица в УЦ в соответствии с пунктом 7 дополнительных требований.



ViPNet HSM



ViPNet HSM

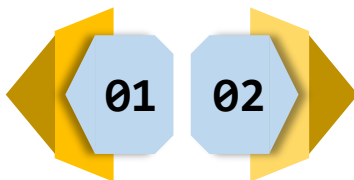


ViPNet HSM

Универсальный
криптографический модуль.

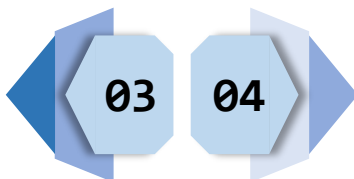
Доверенная криптографическая
платформа.

Программно-аппаратный
модуль
(HSM – Hardware Secure Module)



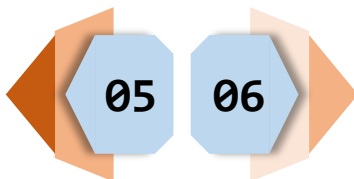
Выполняет криптографические операции по запросам различных сервисов («большой токен»)

Повышенные меры безопасности



Поддержка актуальных криптоалгоритмов

СКЗИ класса КВ

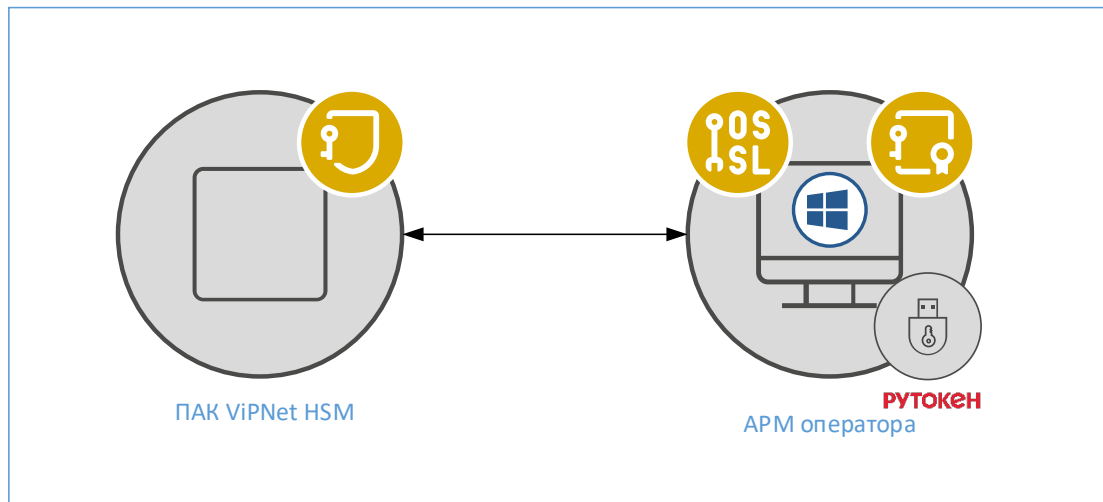


Средство ЭП класса КВ2

ViPNet HSM: подключение прикладных сервисов



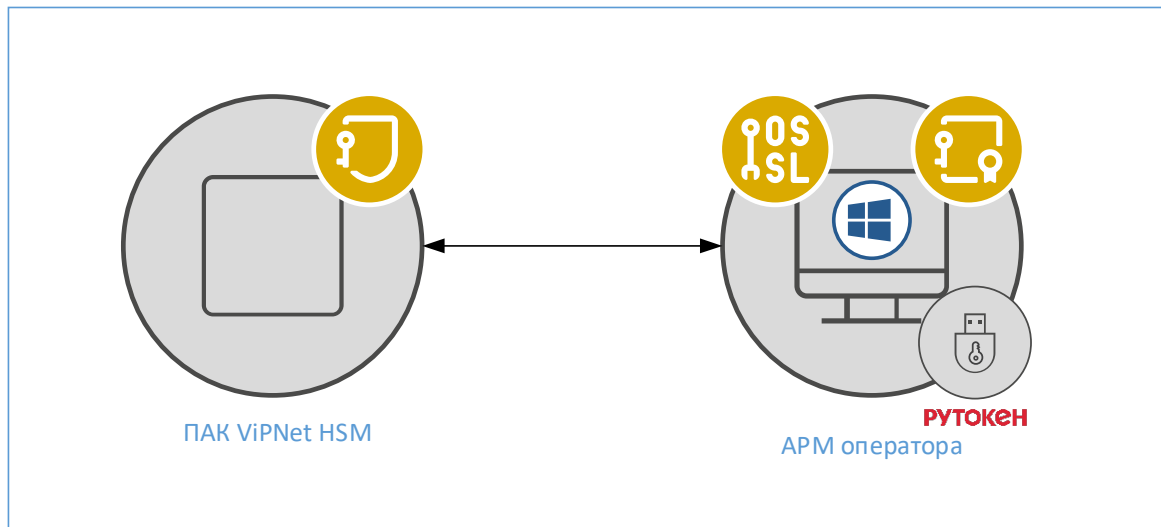
Схема демонстрационного макета



Реализация:

1. Средство ЭП КВ2 – ViPNet HSM.
2. Ключевой носитель – Рутокен ЭЦП 3.0.
3. Средство УЦ – ViPNet УЦ (генерация запроса на сертификат p10 – опционально).

Схема демонстрационного макета



Алгоритм защиты и формат переноса ключей между СКЗИ разных производителей - рекомендации ТК26

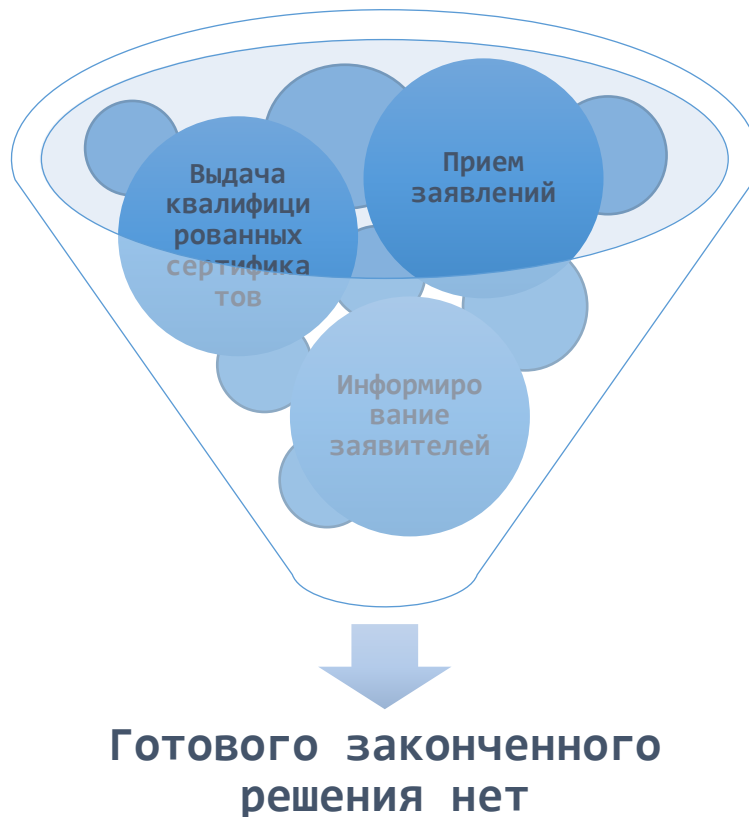


Открытые вопросы



Открытые вопросы

Средство ЭП КВ2 и специализированный ключевой носитель являются компонентами (инструментами) решения, готового решения нет. Сертификация?



Открытые вопросы



Разные вендоры!



Средство ЭП
пользователей,
доработка и
распространение (идет
эксперимент -
безвозмездно от УЦ ФНС
России)



Средство ЭП КВ2

Ключевой носитель 1

Ключевой
носитель
N

Средство ЭП
1пользователя



Средство ЭП
пользователя



Средство ЭП N
пользователя





Спасибо за внимание!

Бадмаева Римма

e-mail: Rimma.Badmaeva@infotecs.ru

Подписывайтесь на наши соцсети



vk.com/infotecs_news



t.me/infotecs_news



rutube.ru/channel/24686363