Алгоритм для выпуска сертификата с ключевой парой КриптоПро CSP в ViPNet УЦ

Версия ПО: JMS 3.4 и новее

Токены: Любые

Проблема:

Нет возможности использовать два криптопровайдера (КриптоПро CSP и ViPNet CSP) на одном сервере JMS для генерации ключевой пары.

Причина:

Необходимость использования криптопровайдера в качестве криптопровайдера уровня ядра, что невозможно с двумя криптопровайдерами на одном сервере.

Решение:

1. Установить второй сервер JMS в качестве узла кластера с подключением к существующей БД.

2. Сформировать запрос и ключевую пару с помощью КриптоПро CSP.

3. На сервере ViPNet УЦ удовлетворить запрос из предыдущего шага по шаблону, включающему следующие политики применения: обеспечение получения идентификации от удалённого компьютера, подтверждение удалённому компьютеру идентификацию Вашего компьютера.

4. Добавить средствами КриптоПро CSP сертификат из предыдущего шага в доверенные сертификаты сервера ViPNet УЦ.

5. В свойствах WebService Server в качестве клиента зарегистрировать этот сертификат.

6. На втором узле кластера JMS установить сертификат средствами КриптоПро в личное хранилище компьютера.

7. Указать сертификат в профиле выпуска КриптоПро CSP в JMS.

Возможен вариант без установки и последующего удаления КриптоПро CSP на ViPNet УЦ (шаг 4): для этого потребуется конвертация контейнера в pfx с помощью КриптоПро CSP или других сторонних средств.

ID статьи: 309

Последнее обновление: 12 Jul, 2019

Ревизия: 1

JaCarta Management System -> Алгоритм для выпуска сертификата с ключевой парой КриптоПро CSP в ViPNet УЦ

https://kbp-6.aladdin-rd.ru/index.php?View=entry&EntryID=309