Вопросы и ответы с вебинара 30 июня 2025 года

«Корпоративный центр сертификации для Linux "Aladdin Enterprise CA" – что нового в импортозамещении Microsoft CA?»

Aladdin Enterprise CA

Страница продукта – https://aladdin-rd.ru/catalog/aladdin-eca/

Запросить демо, пилот, расчет стоимости – question@aladdin.ru

Вопросы - linux@aladdin.ru

1. **Как можно автоматизировать выдачу сертификатов для своих веб-серверов, например, на базе nginx или angie?**

   На текущий момент это можно реализовать через скрипты и через API. Если в вопросе были намеки на поддержку протокола ACME и автоматический выпуск с его помощью, то поддержка протокола планируется ориентировочно к концу 2025 года. Приоритеты могут быть скорректированы по результату совместной проектной работы.

2. **Использование HSM с сертифицированной версией ECA разрешается с ЦС, развернутыми в виртуальной инфраструктуре?**

   Мы обеспечиваем корректность встраивания с СКЗИ КриптоПро CSP классов защиты КС1 и КС2. И ответ зависит от правил использования для данных классов СКЗИ.

3. **Есть ли autoenrollment сертификатов на macOS?**

   Зависит от системы управления устройств на базе macOS. eCA поддерживает протокол SCEP. Насколько известно, устройства macOS используют для получения сертификата именно его.

4. **Есть ли интеграция с РЕД АДМ или ALD Pro??**

   Да. Возможность загрузки объектов каталога и его свойств и оперативное обновление (сотни тысяч объектов). Возможность выпуска сертификатов для объектов и публикация сертификата в каталог. Возможность организации строгой аутентификации в домене, т.е. по сертификатам. Возможность публикации списков отзыва. И на 2025 год планируем более тесную интеграцию, в том числе связанную с доменными политиками.

5. **А разве сейчас актуально Microsoft, как же полный переход на отечественное ПО Astra Linux?**

   Переход на отечественное ПО в части клиентских компьютеров не произойдет за один год. Текущие инфраструктуры в огромных количествах используют ПО на базе Microsoft.

6. **Можно ли как-то с помощью политик настроить ограничения по маске на альтернативные имена в шаблоне выпуска сертификатов. Например, на шаблоны с клиентской и серверной аутентификацией? Для предотвращения повышения полномочий в домене.**

   Нет, на текущий момент данный функционал не поддерживается. Для предотвращения несанкционированного повышения полномочий мы используем механизм, в котором пользователь может запросить сертификаты только для своей УЗ. Эту задачу можно включить в план работ, предлагаем связаться с нами для её уточнения.

7. **При оказании услуг по выпуску сертификатов для разных организаций, реализован ли биллинг в eCA для таких сценариев применения?**

   Биллинг не реализован и на данный момент не запланирован. При этом для Multitenancy сделано многое, например, работа с несколькими доменами, издателями, делегирование полномочий и т.д. Предлагаем обратиться к нам для уточнения задачи.

8. **Есть ли возможность выпускать сертификаты ГОСТ и RSA на одном подчиненном ЦС?**

   Видимо имеется ввиду на одном сервере. Да, технически такая возможность имеется.

9. **Можно ли использовать носители других производителей, например, Рутокен?**

   RuToken поддерживается в решении для централизованного управления ключевыми носителями JaCarta Management System. Поддержка RuToken в Aladdin eCA возможна. На 2025 год мы рассматриваем возможность реализации этой возможности. Предлагаем обратиться для уточнения деталей.

10. **Что делать после того, как закончится срок действия перенесенного корневого сертификата Windows?**

    Создавать новую PKI инфраструктуру. Если истек корневой сертификат, то путь только один. Создавать новую инфраструктуру со всеми сопутствующими мероприятиями.

11. **Доверительные отношения между доменами — это будет реализовано?**

Двухсторонние доверительные отношения поддерживаются самими доменами. Если мы неправильно поняли вопрос, напишите нам.

12. **Расскажите, как продукт прошел сертификацию?**

Успешно.

13. **Для Центра Регистрации планируется ли добавить поддержку OpenID Connect\SAML**

Рассматриваем возможность реализации поддержки к концу 2025 года. Для уточнения задачи и если необходимо – корректировки приоритетов предлагаем связаться с нами для уточнения задачи.

14. **Могу ли я задать доменную группу в шаблоне для автоэнролла?**

Да

15. **Вопрос о резервном копировании, как бекапить корневой ЦС?**

Описания процессов создания резервной копии содержится в руководстве администратора.

16. **SAN помимо DNS, что еще поддерживается и какое количество записей?**

- RFC 822 Name
- DNS Name
- IP address
- Directory Name
- Uniform resource identifier
- Registered Identifier (OID)
- MS UPN, User Principal Name
- MS GUID, Globally Unique Identifier
- Kerberos KPN, Kerberos 5 Principal Name
- Permanent Identifier
- Xmpp address

- Service Name
- Subject Identification Method

17. А где acl у шаблона? Кому энроллить будем?

ACL для шаблона — это правила выпуска в компоненте «Центр регистрации»

18. Могу ли я задать доменную группу в шаблоне для автоэнролла?

Да

19. По какому классу сертифицируетесь в ФСБ?

В настоящее время не рассматриваем задачу проходить сертификацию на соответствие 796 приказу ФСБ как Средство УЦ