

Как вычислить ответ на запрос при инициализации JaCarta PKI с установленным 3DES ключом

Версия ПО: EK 2.6.x.x - 2.7.x.x, JC-Client 6.x

Токены: JaCarta PKI и PKI/BIO

Проблема:

После персонализации JaCarta PKI через JMS с заданным параметром "запрос-ответ" невозможно инициализировать ключевой носитель на другой рабочей станции при помощи EK или JC-Client.

Причина:

Инициализация ключевого носителя с предустановленной опцией "запрос-ответ" в EK или JC-Client возможна только посредством ввода ответа, который вычисляется калькулятором через значение 3DES ключа, которое должно быть известно. Это значение указано в шаблоне инициализации ключевых носителей в JMS. По умолчанию это значение "00000000".

Решение:

- При инициализации через EK или JC-Client в окне инициализации присутствует два поля - "Запрос" и "Ответ", в поле "Запрос" присутствует строка вида "d76adf87ddf876df". Для вычисления ответа можно использовать любой 3DES калькулятор (например, DESUtil).

- В поле "Key" необходимо вписать ASCII значение пин-кода администратора смарт-карты, переведённое в HEX формат. Получить это значение можно любым онлайн калькулятором ASCII to HEX. Далее в результате подсчета нужно удалить символы вида «0x», или выбрать опцию «Remove 0x». Если в шаблоне JMS значение "00000000", то в HEX это равно "3030303030303030".

- В поле "Data" необходимо подставить значение из поля "Запрос" окна инициализации.

- Нажать "Encrypt", после чего в поле "Result" появится значение вида "e903f40c454cf540", которое нужно подставить в поле "Ответ" в окне инициализации. При верном вводе всех параметров инициализация пройдет успешно.

После каждого неверного ввода значения "Ответ" значение поля "Запрос" меняется.

Утилита DESUtil доступна по ссылке:

[/kb_upload/file/DESUtil.zip](#)

JaCarta -> Как вычислить ответ на запрос при инициализации JaCarta PKI с установленным 3DES ключом

<https://kbp-6.aladdin-rd.ru/index.php?View=entry&EntryID=68>