Двухфакторная аутентификация в доменной инфраструктуре ОС Альт. Общая информация.

Служба обеспечения совместимости <gost@basealt.ru>, Константин Белаш

Version 1.3, 01.07.2022

Оглавление

1. Об этом документе

Настоящий документ можно считать вводным руководством для конечного пользователя с теоретическим описанием работы двухфакторной аутентификации (2ФА) в доменной инфрастуктуре.

Из этого документа станет понятно, как работает 2ФА в домене Samba DC, FreeIPA или Windows AD, где в качестве клиента выступает ОС «Альт Рабочая станция 10».

Документ необходимо использовать в дополнении к практическому руководству по настройке 2ФА для конкретной доменной инфраструктуры.

2. Общая схема работы доменной 2ФА

Двухфакторная аутентификация (2ФА, 2FA) — это метод идентификации пользователя в каком-либо сервисе при помощи запроса аутентификационных данных двух разных типов. Суть 2ФА: чтобы куда-то попасть, необходимо подтвердить тот факт, что вы — это вы, причём при помощи двух факторов («ключей»), одним из которых вы владеете, а другой знаете (держите в памяти).

Совместно токен и PIN-код формируют такую систему 2ФА: токен — «ключ», которым вы владеете, а PIN-код к нему — «ключ», который вы знаете, т.е. в данном случае: 1-й фактор — наличие сертификата пользователя на токене, выданного Удостоверяющим Центром (УЦ) сертификации, а 2-й фактор — наличие доступа к сертификату пользователя на токене (владение) — знание PIN-кода.

Процедура аутентификации пользователя в домене при использовании сертификата на токене (смарт-карте):

1. предъявляется имя пользователя (в консоли или менеджеру входа в систему)
2. PAM-модуль (pam_sss) и служба sssd проверяют для этого имени пользователя доступность аутентификации по токену, а именно:
    a. сертификат на токене выпущен УЦ, которому мы доверяем
    b. сертфикат действителен, т.е. не отозван
    c. можно ли однозначно сопоставить доменного пользователя и сертификат
        i. по умолчанию проверяется соответствие сертификата на токене и сертификата в базе LDAP домена для этого пользователя
        ii. если сертификата в базе LDAP домена нет, то сопоставление производится согласно правилу `maprule` службы sssd
3. при успешном сопоставлении сертификата и доменного пользователя запускается процесс PKINIT
    a. выдаётся запрос на ввод PIN-кода
    b. если PIN-код корректный, то проверяется соответствие всей цепочки сертификатов: пользователя, домена (KDC, Центр распределения ключей) и УЦ
    c. если цепочка сертификатов успешно проверена, то пользователю выдаётся билет Kerberos и осуществляется вход в ОС
4. если проверки не пройдены и существует альтернативный способ аутентификации, предлагается им воспользоваться, иначе вход в ОС отвергается

PKINIT — это механизм предварительной аутентификации (до приглашения ввести пароль) для Kerberos 5, который использует сертификаты X.509 для аутентификации клиентов в доменной инфраструктуре.

3. Какие ОС используем для настройки

Для настройки используется ОС с менеджером входа в систему LightDM для «Альт Рабочая станция 10» или SDDM для «Альт Рабочая станция К 10». В качестве контроллера домена Samba DC или FreeIPA используется ОС «Альт Сервер 10». В качестве домена Windows AD используется «Windows Server 2012R2» либо «Windows Server 2019».

4. Какие токены используем для настройки

Для настройки используем токены с аппаратной поддержкой криптографических функций. В таких токенах приватный ключ генерируется непосредственно на токене и является неизвлекаемым. В этом случае администратор инфраструктуры PKI может быть уверен, что для 2ФА приватный ключ на токене, на основе которого получен сертификат, не может быть каким-либо образом скопирован или размножен, в отличие от обычных токенов, где контейнер с криптографической информацией может быть скопирован на другой токен и в таком случае одного фактора система 2ФА будет лишена.

Перечень подходящих токенов можно посмотреть в документе «Методика тестирования токенов» (доступна по запросу в службу обеспечения совместимости).

5. Какие протоколы шифрования используем

Для настройки доменной 2ФА используется протокол шифрования RSA. Он выбран из-за поддержки всеми компонентами, участвующими в процессе 2ФА, а именно:

- библиотеки вендоров pkcs11;
- openssl engine (engine, который позволяет работать с токеном, а не тот openssl-gost-engine, который может работать с протоколами ГОСТ, но без токена);
- служба аутентификации sssd;
- Kerberos PKINIT;
- Удостоверяющий Центр (сертификации).

Отечественные протоколы шифрования ГОСТ поддерживаются библиотеками вендоров pkcs11, но openssl engine и PAM-модуль, с поддержкой протоколов ГОСТ, свободно предоставляются только компанией Актив для своих токенов (Рутокен). Служба аутентификации sssd и MIT Kerberos протоколы шифрования ГОСТ не поддерживают.

6. Предварительные условия для использования токенов и смарт-карт

Перед настройкой доменной 2ФА необходимо убедиться, что токены корректно взаимодействуют с ОС по протоколу PC/SC, а также поддерживается функционал библиотек вендоров PKCS#11. Сделать это можно в соответствии с отдельным документом «Методика тестирования токенов» (доступен по запросу в службу обеспечения совместимости).

7. Приложение

7.1. Проверка количества попыток ввода пин-кода

При успешной 2ФА, как следствие корректного ввода пин-кода для токена, количество попыток ввода пин-кода сбрасывается к первоначально заданному значению.

Если нужно проверить, что после успешной 2ФА количество попыток соответствует максимально возможному и дополнительных (несанкционированных) обращений к токену без указания корректного пин-кода нет, то необходимо воспользоваться утилитами ведоров токенов, которые показывают данные значения.

Следует учитывать, что при неверном вводе пин-кода счетчик попыток всегда уменьшается.

Количество неверных попыток ввода пин-кода устанавливается, как правило, при форматировании (инициализации) токена.

7.1.1. Рутокен ECP

Для получения количества оставшихся попыток ввода пин-кода используем утилиту `GeneralPurpose_Active` (в открытом доступе её нет, можно запросить у вендора).

После успешной 2ФА в пространстве доменного пользователя выполняем:

```
rt_win@work ~ $ /opt/GeneralPurpose_Active
Initialization...
 LoadLibrary -> OK
 GetProcAddress -> OK
 GetProcAddress -> OK
 Get function list -> OK
 Get function list extended -> OK
 C_Initialize -> OK
 C_GetSlotList (number of slots) -> OK
 Checking available tokens -> OK
 Memory allocation for slots -> OK
 C_GetSlotList -> OK
 Slots available: 1
Initialization has been completed successfully.

Getting extended token information...
 C_EX_GetTokenInfoExtended -> OK
Extended token information has been got successfully.

Extended information:
 Token class:                0x00000001 (Rutoken ECP)
 Protocol number:            0x00000001
 Microcode number:           0x00000017
 Order number:               0x00000002
```

```
 Flags:                        0x00000c03
 Max admin PIN length:         32
 Min admin PIN length:         6
 Max user PIN length:          32
 Min user PIN length:          6
 Max admin retry counter:      10
 Admin retry counter:          10
 Max user retry counter:       10
 User retry counter:           10
 Serial number:                00 00 00 00 3C E9 67 75
 Total memory:                 0x00010000
 Free memory:                  0x0000acc0
 ATR:                          3B 8B 01 52 75 74 6F 6B 65 6E 20 44 53 20 C1
 Token class:                  0x00000001
 Battery voltage (Bluetooth): 0x00000000
 BodyColor (Bluetooth):        0x00000000
 Firmware checksum:            0xc911a7a7

Extended info test has been completed successfully.

Finalizing...
 C_Finalize -> OK
 FreeLibrary -> OK

Sample has been completed successfully.
```

Здесь нас интересует 2 параметра: `Max user retry counter` и `User retry counter`.

- `Max user retry counter` — максимально возможное количество попыток ввода пин-кода для пользователя
- `User retry counter` — количество оставшихся попыток ввода пин-кода для пользователя

7.1.2. JaCarta

Для токенов компании Аладдин воспользуемся `Единый Клиент JaCarta` (https://www.aladdin-rd.ru/support/downloads/jacarta_client).

- ПК «Единый Клиент JaCarta 2.13» (версия для Alt 8, 9)
- ПК «Единый Клиент JaCarta 3.0» (версия для Alt 10, в разработке)

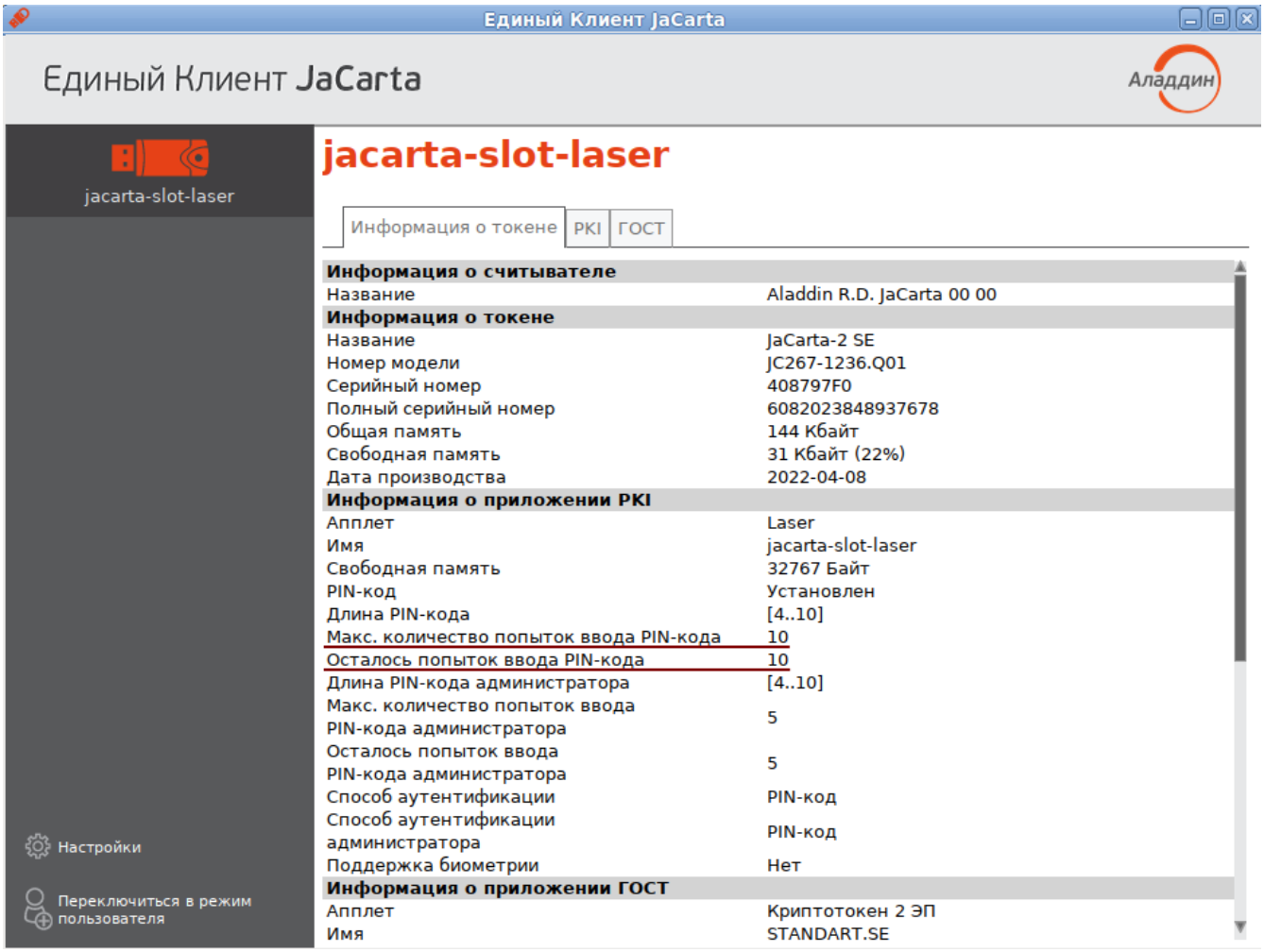
Прежде чем установить «Единый Клиент JaCarta», необходимо удалить `libjcpkcs11`.

```
# apt-get update
# apt-get dist-upgrade
# apt-get remove libjcpkcs11
# apt-get install ./jacartauc_2.13.11.3194_alt_x64.rpm \
./jcpkcs11-2_2.7.4.540_alt_x64.rpm
```

После успешной 2ФА в пространстве доменного пользователя выполняем:

- Открываем `Единый Клиент JaCarta`: Приложения → Стандартные → Единый Клиент JaCarta
- Переключаемся в режим администратора
- Выбираем вкладку «Информация о токене» → раздел «Информация о приложении PKI»

Здесь нас интересует два параметра: `Макс. количество попыток ввода PIN-кода` и `Осталось попыток ввода PIN-кода`:



7.1.3. ESMART Token

Для токенов компании ISBC воспользуемся утилитой `PKIClientCli`.

Установка утилиты:

```
# apt-get install isbc-pkcs11-utils
```

После успешной 2ФА в пространстве доменного пользователя выполняем:

```
# PKIClientCli listslots
Slot 1: ESMART Token GOST [ESMART Token] (ESMART Token GOST [ESMART Token] 00 00)
    token label         :esmart_64
```

```
    token manufacturer  :ISBC
    token model         :ESMART Token
    serial num      :206F6060C102
    HW version      :0.0
    FW version      :2.0
    PIN attempts        :10
    SOPIN attempts      :10
```

`PIN attempts` — количество оставшихся попыток.