Павел Волнейкин

Аутентификация по аппаратным токенам в дистрибутивах Альт

Поддержка токенов. Статус

- Работают различные модели отечественных токенов. В том числе — совместно.
- С их помощью можно выполнять аутентификацию.
- Простая настройка через Альтератор.
- Автоматическое создание учётных записей.
- Доступно в репозиториях P8 и Сизиф.

Состав ПО

- Модуль аутентификации — **pam_pkcs11.so**.
- Криптографическая библиотека **libcrypto.so** (OpenSSL).
- Способы шифрования (engines).
- Модули доступа к токену (различные реализации PKCS#11).
- Модули проекции данных токена на имена пользователей (mapping).
- Служба PC/SC (низкоуровневый доступ к токену).

Состав ПО (окончание)

- Отслеживание событий (вставка и извлечение токена) — **pkcs11_eventmgr**.
- Скрипты — обработчики событий.
- Контроллер пользовательских сеансов (**loginctl**).
- Гритер — диалог входа в систему.
- Хранитель (блокировщик) экрана.

Категории параметров конфигурации

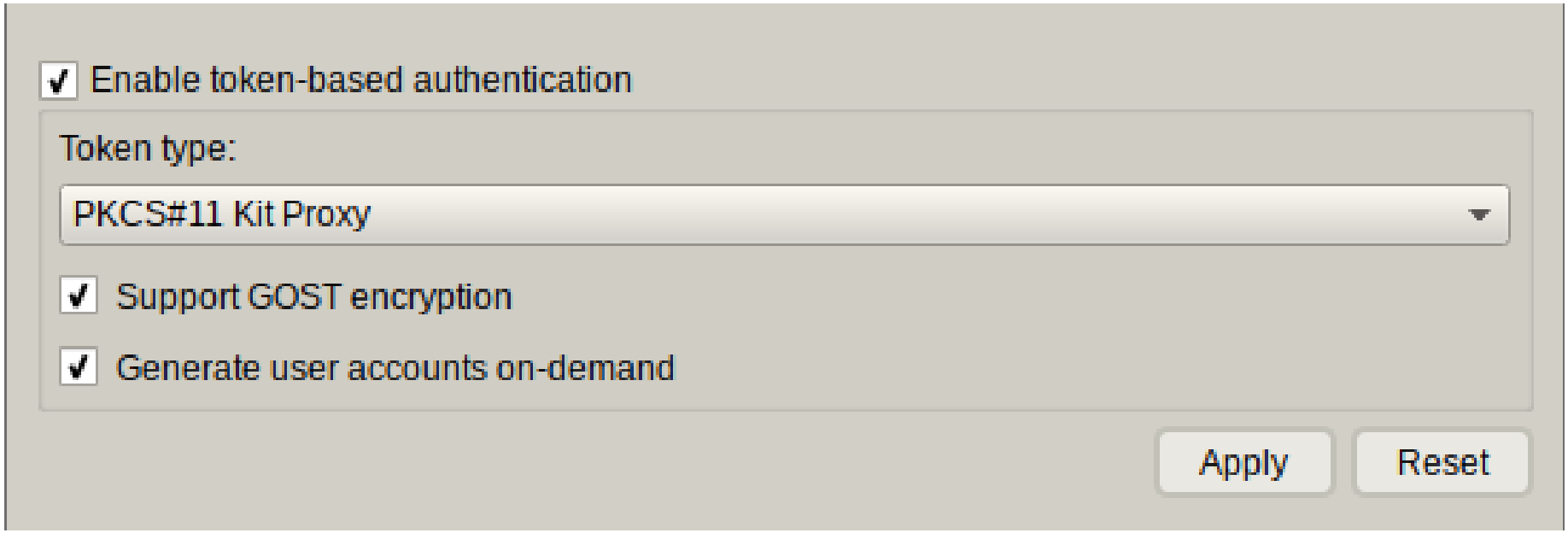
- Взаимодействие с определённой моделью токенов — выбор модуля PKCS#11.
- Способ отображения сертификатов на имена пользователей.
- Доверие и проверка сертификатов.
- Прочие параметры PKCS#11 (ожидание подключения, запрос PIN-кода и т. п.).
- Политика входа в систему (без использования токена / с обязательным использованием токена и т. д.).

Категории параметров конфигурации (окончание)

- Отслеживание состояния токена и реакция на события.
- Настройка автоматической регистрации учётных записей.

*Все указанные группы параметров доступны для управления через **control**.*

alterator-auth-token



Преднастройка в Alterator

```
[Desktop Entry]
Type=Application
Categories=X-Alterator-Users
Icon=auth-token
Terminal=false
Name=Hardware token and smart-card authentication
X-Alterator-URI=/auth-token?profile=rutokenecp&gost=1&autoadd=1
X-Alterator-Weight=30
X-Alterator-Help=auth-token
Name[ru]=Аутентификация по аппаратным токенам и смарт-картам
```

Типовая настройка

- Аутентификация рядовых пользователей только по токену.
- Блокировка сеанса при извлечении токена.
- Признак учётной записи — наличие сертификата в домашней директории пользователя.
- Доверие сертификатам УЦ из **ca-gost-certificates**.

Автоматическая регистрация учётных записей

- Произвольный OID в качестве основной части имени пользователя.
- Возможность её замены на хеш-сумму (SHA1) в Base64 (почти).
- Имя пользователя: **префикс-XXXX-суффикс.**

Автоматическая регистрация учётных записей (типовая)

- СНИЛС в качестве уникального идентификатора.
- Попытка спрятать СНИЛС за хеш-суммой.
- Имя пользователя вида **auto-HHHHHH-snils**.