eToken PASS

Назначение

Автономный генератор одноразовых паролей eToken PASS (Синхронизация по событию, Синхронизация по времени) можно использовать для аутентификации в любых приложениях и службах, поддерживающих протокол аутентификации RADIUS – VPN, Microsoft ISA, Microsoft IIS, Outlook Web Access и др.

Комплект разработчика eToken OTP SDK 2.0 позволяет легко добавить поддержку аутентификации по одноразовым паролям в собственные приложения.

Принцип работы

В eToken PASS реализован алгоритм генерации одноразовых паролей (One-Time Password – OTP), разработанный в рамках инициативы OATH. Этот алгоритм основан на алгоритме HMAC и хэш-функции SHA-1. Для расчета значения OTP принимаются два входных параметра – секретный ключ (начальное значение для генератора) и текущее значение счетчика (количество необходимых циклов генерации). Начальное значение хранится как в самом устройстве, так и на сервере в системе eToken TMS. Счетчик в устройстве увеличивается при каждой генерации OTP, на сервере – при каждой удачной аутентификации по OTP.

При запросе на аутентификацию проверка OTP осуществляется сервером RADIUS (Microsoft IAS, FreeRadius и другие), который обращается к системе SafeNet Authentication Manager (SAM), осуществляющей генерацию OTP на стороне сервера. Если введенное пользователем значение OTP, совпадает со значением, полученным на сервере, аутентификация считается успешной, и RADIUS сервер отправляет соответствующий ответ.

Партия устройств eToken PASS поставляется с зашифрованным файлом, содержащим начальные значения для всех устройств партии. Этот файл импортируется администратором в систему SafeNet Authentication Manager (SAM). После этого для назначения устройства пользователю необходим ввод его серийного номера (печатается на корпусе устройства).

Преимущества

·Не требует установки дополнительного клиентского ПО.
·Не требует установки драйверов.
·Работает без подключения к компьютеру – нет необходимости наличия свободного USB-порта.
·Возможность работы в любой операционной системе.
·Возможность работы с мобильных устройств.
·Одноразовый пароль действует только в течение одного сеанса связи – пользователь может не беспокоиться о том, что пароль может быть подсмотрен или перехвачен.
·Низкая цена.

В случае нарушения синхронизации счетчика генерации в устройстве и на сервере, система SafeNet Authentication Manager (SAM) позволяет легко восстановить синхронизацию – привести значение на сервере в соответствие значению, хранящемуся в устройстве. Для этого администратор системы или сам пользователь (при наличии соответствующих разрешений) должен сгенерировать два последовательных значения OTP и отправить их на сервер через Web-интерфейс SafeNet Authentication Manager (SAM).
В целях усиления безопасности система SafeNet Authentication Manager (SAM) позволяет использовать дополнительное значение OTP PIN – в этом случае для аутентификации пользователь помимо имени пользователя и OTP вводит дополнительное секретное значение OTP PIN. Это значение задается при назначении устройства пользователю.

Модификации

·Цветная печать на поверхности.
·Нанесение логотипа на корпус.

2009 SC Magazine «Best Buy» 5-Star Rating

Network Product Guide's Best in Tokens

2009 WindowSecurity.com Reader's Choice 1st Runner Up

Платиновый партнер SafeNet Inc. в Казахстане

AkNur Security
г. Алматы, ул. Егизбаева 13, офис 4
тел: +7 (727) 394 05 50, 394 06 09
e-mail: info@aknur.kz
www.aknur.kz