Общий FAQ по использованию устройства.

Q: Я потерял устройство. Другой его нашел. Что делать?
A: Моделей защиты несколько, они будут выбиратся:

1. Пароли на устройстве создаются “на лету” из пин-кода пользователя и внутреннего ключа при помощи алгоритмов хеширования. То есть от каждого возможного пин-кода будет свой пароль. Нашедший устройство просто не будет знать, какой пин-кода верный, устройство для всех пин-кодов отдает пароли, но для неверного пин-кода будет и пароль неправильный. Эта модель позволяет иметь несколько банок паролей на одном устройстве, вводя разные пин-коды.
2. Тоже самое, что в п.1, но ключа уже два: для правильного пин-кода и для остальных. Дополнительно в устройстве сохраняется хеш правильного пин-кода. Дальше, например, при 4 попытках неверного ввода устройство изменит ключ правильного пин-кода, от которого создавались пароли - даже если злоумышленник угадает пин-код перебором, пароли он получит неправильные.
3. Просто пин-код и 3 попытки его ввода. Не угадал - ключ стерся.

Q: Меня взяли за задницу преступники, и они просят пин-код. Что делать?
A: Устройство имеет пин-коды для полного стирания памяти. Их набор гарантированно сменит пароли, после чего можно будет отдать настоящий пин-код - твоих паролей там не будет, да и привязка к облаку отвалится. Если такое устройство попробовать синхронизировать без сброса в аккаунте - бекап будет заблокирован.

Q: У меня в почте зашифрованная переписка, содержащая неоднозначные или не одобряемые обществом вещи. Кто-то из родственников может знать мой пин-код, подсмотрев набор. Как быть?
A: Устройство поддерживает динамические пин-коды:

1. Каждый раз разный пин-код, метод генерации которого задается в настройках. *Например, сегодня 1.01 и пинкод будет 777101, а завтра он будет 777201. Пусть подглядывают.*
2. Пин-код из большого набора изображений, из которых надо выделить тег. *Например, 16 картинок котят, в которых надо тапнуть по порядку только белых с черным пятном. Поскольку никто не знает, по какому принципу идет выборка котят, отгадать такой пин-код подсмотревшему почти невозможно - картинок котят всего 256 штук и выводятся они случайно по 16 штук.*

Q: Я укурился\набухался и боюсь, что начну использовать устройство в нетрезвом виде. Как быть?
A: Устройство имеет временную блокировку от использования. Устройство отключается специальным пин-кодом и восстанавливается только в установленное время после синхронизации с облаком.

Q: Я имею очень важные или секретные данные, которые даже зашифрованными нельзя класть в облако. Как быть?
A: Устройство имеет несколько уровней безопасности:

1. Параноидальный. Динамический пин-код с двумя попытками ввода. Синхронизация с облаком отключена, ключ шифрования памяти использует пин-код и внутренний ключ. Флешка дополнительно запаролена аппаратно, то есть снять с нее даже зашифрованный бекап нельзя - для любого другого устройства она выглядит как неисправная. При любой тревоге (введен пин-код стирания, неверный ввод пин-кода) происходит не только стирание ключей, но и полный снос прошивки, а также стирание карты. Если с устройством что-то случилось - восстановление базы невозможно.
2. Максимальный. В нем дается три попытки на ввод пин-кода, синхронизация с облаком отключена, ключ шифрования памяти использует пин-код и внутренний ключ. Взлом такого устройства невозможен даже с использованием человеческого фактора, однако поломка, утеря или сбой приведут к полной потере всего содержимого. Бекапить флешку тоже бесполезно, так как ключ от нее будет неизвлекаемым.
3. Средний. Файлы в облаке зашифрованы на хеш от пин-кода пользователя, память тоже. Внутренний ключ для шифрования не используется. При утере, порче или сбое устройство легко восстановить, однако хищение пин-кода даст возможность взлома базы.

Q: Я слышал, что можно прочесть память контроллера через технологические режимы или баги в реализации бит защиты...
A: Информации о взломе STM32F4 нет, и скорее всего, бекдор тоже не существует. Прочитать память можно, но делают это в десятке лабораторий в мире, стоить это будет сотни тысяч долларов, да и у атакующего будет одна попытка с вероятностью успеха процентов в 25. Можно считать, что устройства достаточно защищены для использования на гражданке.