Общий FAQ по техническому устройству.

Q: Можно ли приделать сканер отпечатков?
A: Можно. Однако есть проблемы.

1. Сканеров свободного назначения в продаже как-то не густо, и почти все они - огромные по размерам, предназначенные для установки на объектовых КПП. От телефонов поставить нельзя, документацию на него нам никто не даст, а без документации для написания драйверов это просто кусок пластмассы.
2. Безопасность бытовых сканеров отпечатков нулевая. Подделать отпечаток при наличии навыков задача очень простая.
3. Сканер отдает картинку. Обработка и сравнение отпечатка - очень сложная высшая математика, кода очень много. Часть можно взять из библиотек линукса, но в любом случае работы там очень много.

Q: Можно ли заменить нашим устройством токены для банк-клиентов?
A: Теоретически да. Технически все необходимое там есть. Но для такого токена нужна сертификация и куча лицензий от всех возможных регуляторов - иначе банк справедливо пошлет лесом самоделкиных.
Основа банковских токенов - доверие разработчику и ЦС. Рынок очень закрытый и консервативный по понятным причинам - какое доверие на проходном дворе? На старте сюда лезть полностью бесполезно.

Q: Почему нужно отдельное устройство? Почему не сделать приложение на телефон?
A: Несколько проблем.

1. На андроид сделать такое приложение можно. Но для него нужен рут и сборка драйверов под конкретное ядро (то есть под конкретную модель телефона). Гемор страшный. На остальные устройства такое прикрутить нельзя.
2. Телефоны дырявы насквозь, и по ним не шарится только совсем ленивый. Даже для брендов, исключая разве что Apple, драйвера пишет индус за доллар в день - качество там ниже плинтуса, ехала уязвимость через уязвимость. Хакеры и спецслужбы могут отломить любой телефон и угнать базу паролей при первом желании. Какой смысл держать пароли в таком ненадежном месте?

Q: Зачем карта памяти? Почему не nand/eMMC?
A: Во-первых, хранить пароли, кошельки, другую инфу. Даже если устройство навернулось, мы можем переставить карту в другое и продолжать пользоваться. Данные зашифрованы, и такая операция безопасна. Во-вторых, карта стоит дешевле той же eMMC аналогичного размера, и на прототипах куда проще поставить карту, а не паять BGA.

Q: Сколько паролей влезает?
A: Для версий с картой - сколько угодно. Для простой версии - по количеству кнопок.

Q: Везде ли поддерживается?
A: Да, везде. По крайней мере там, где есть поддержка USB HID - а это любое устройство: телефон, игровая приставка, ТВ-приставка, ПК, Raspberry Pi, и прочее оборудование. Надо уточнять, однако, насчет телефонов Apple - возможно, нужен будет специальный переходник.

Q: Что понимать под поддержкой?
A: Принцип “устройство как сервис”

1. Есть две прошивки - одна открытая от сообщества, другая фирменная. Технически они почти одинаковы, но та, которая открытая, с официальными серверами не синхронизируется. Можно поднять свой сервер, но это реально будут делать 1 из 10 тысяч.
2. Синхронизация официальных устройств с сервером. Там хранится зашифрованная на пароль пользователя база, и ее кража для хакеров полностью бессмысленна.
3. Создание и поддержка SDK для написания приложений под официальную версию - чтобы самим не морочить голову написанием кошельков для криптовалют.
4. Приложения под все мобильные платформы и на десктоп.

Q: Какой функционал планируется в идеале?
A: Большой =)

1. Аппаратный менеджер паролей
2. Имитатор CD-ROM для установки ОС (если позволит скорость чипа)
3. Маленькая защищенная флешка
4. Неизвлекаемое хранилище
5. Цифровая подпись, совместимая с OpenSSL
6. Шифрование RSA и AES для различных нужд
7. TOTP
8. Криптовалютные кошельки
9. Тамагочи (шутка)

Q: А че такой похабный экран? Где IPS?
A: Хороших экранов в рознице нет, видимо, они поштучно никому не нужны. Все хорошие дисплеи от 4 дюймов размером, что для нашего устройства перебор. Есть маленькие oled, но стоят они очень дорого и не комплектуются сенсорными панелями. Если взлетит - можно поковырять алибабу и поискать приличный дисплей, сейчас обойдемся обычным TFT.

Q: Можно ли заказать 2-3 штуки плат для тестов?
A: Можно. Но сэкономить не выйдет.

1. Платы что 2, что 10 стоят одинаково 2 бакса
2. Под плату нужен трафарет, стальной лист 20 x 30. Без него запайка превращается в производство брака. Я с трудом запаял без трафарета маленькую версию, большую вообще не реально запаять, не перегрев всё подряд.
3. Заказ делается неделю и идет месяц-полтора.

UPD 31-05-18: Платы и трафареты подешевели, комплект с доставкой стоит $20.

Q: Не украдут ли китайцы? Какую защиту прикрутить?
A: Обязательно украдут. Это неизбежно и сделать ничего нельзя: чувак на хабре вон ради шутки сделал абсолютно бесполезный usb-killer для порчи портов - так через год оно на али появилось в куче мест. Зачем? Китаец увидел - китаец сделал, а рынок сам определит зачем. Потому надо изначально понять, как от китайских клонов получить выгоду, а не убыток. Прикручивать защиту бесполезно, даже вредно: китаец просто сделает аналог, а не клон, и тогда профит с него не поиметь никак.

Q: Что такое индексы A, B, C у MeW Pro?
A: Плата изначально была запроектирована универсальной. Различия такие:

1. Модель A. Максимальная, есть все оборудование. **Эта модель основная.**
2. Модель B. Без батареи и с более слабым контроллером (но незначительно). Батарея не сильно нужна в большинстве применений такого устройства, потому аппарат без нее имеет право на существование.
3. Модель C. Это модель B, но без bluetooth. Опять же, многим он не нужен.