17Shopping.com Crypto Currency Hardware Wallet

Version One High Level Product Specification 0.3 @ April 28th, 2018

The document briefly describes high level hardware, software and functional specification for 17shopping.com cold wallet product code name Version One.

Overview

Version One's market position target for crypto currency trader and owner who seeking for high secure, physical hardware secured wallet to store different types (max. To 5 for now, TBD) crypto currencies, the device with screen and navigation buttons to display and process transaction once connect with laptop, pc or mobile devices.

High level functional specification

- Version One is a "cold wallet" use for store, access and operate crypto currency's "private key" on separate, secured hardware isolated from connected world.
    - Crypto currency: specific mean private key(s) that represent crypto currency's value.
    - Store: able to receive and store specific private key in secured, static location, include but not only in secured memory in 17shopping Version One hardware
    - Operate: able to work with selected hot wallet, web wallet to do to below operation - create unsigned transaction by hot wallet, sign the transaction by 17shopping Version One, send the signed transaction for broadcast.
    - Access: physical connection between Version One hardware and hot wallet for store and operation

Hardware specification

- Form factor
    - Bar type, non-touch 2.0-inch IPS display with 12 key number keypad and one separate hardware button.
- Hardware
    - Dimension: 100mm x 70mm x 7mm
    - Weight: TBD

    - Display: 2.0-inch IPS display, full color, 320x480 pixels
        - AML-FRD200H30100-A
        - Transmissive type a-Si TFT-LED module with white LEDx3 backlight driver circuit (ST7789V)
        - 2.0-inch screen size
        - RGB (262K) with resolution 240x320mm
        - Sleep and stand-by mode available.
        - Partial-screen display function
    - (TBD) Micro-controller: STM32L476xx
        - *FreeRTOS* as operation system on top of STM32L476
    - (TBD) Security Element: Infineon SLE97
    - (TBD): Key: 12 key number keypad with two symbol keys, separate power on/off toggle key
    - Connection: USB Type-C connector
        - (TBD)USB class support: 00h(device), 03h(HID), 05h(Physical),
        - (TBD) Additional class: 07h(printer), 08h(Smartcard), ODh(content security)
    - Certification level CC EAL5+
- User interface
    - On device menu-based user interface for information access, operate and store.
        - Physical key layouts for input and navigator
        - Power on/off key for power cycle
        - 2.0-inch screen for information display
    - USB Type-C connector between Version One and hot wallet device for transaction.

<u>Software specification</u>

- On device software
    - Operation system support function and activities on power cycle
    - UI framework able to complete on device menu and function
    - API (or command set) for hot wallet connect from external target machine to secure element in Version One hardware
    - Housekeeping and maintain function

- Companion software on laptop, mobile.
    - Device driver: connect V1 to external target machine, include and not limited to Personal Computer, mobile device and web browsers
        - (TBD) Microsoft Windows 7 and higher, Intel processor-based device.
        - (TBD) MacOS 10.x or higher, Intel processor-based device.
        - (TBD) iOS 9.x and higher Apple devices
        - (TBD) Android 6.0 and higher mobile devices, limited support with whitelist (will update compatible list in regular basis)
        - (TBD) Chrome and Firefox on desktop operation system with level of security enabled.
    - Device manager: manager app to manage, operate hardware wallet
        - Device firmware updater
            - Provide interface and function to get updated firmware and security patch for Version One product
            - Able to launch once user connect Version One with desktop or mobile device automatically
            - Able to auto-check device serial number, device type, device status and firmware version.
            - Able to verify device’s integrity based on checksum (CRC32 or MD5 checksum) or hardware serial number.
            - Able to verify secure element’s integrity
            - Able to auto-check latest firmware on OTA server based on device type, status and firmware version
            - Able to launch firmware upgrade process on laptop/mobile device and download latest firmware
            - Able to process secure firmware update
            - Able to verify installed firmware, backup firmware and data

        - Device application updater: Able to manage, add, delete, enable, disable application on device's platform, in here the application include (but not limited to) crypto currency "Wallet" running on McU and SE, exchange-specific application and generic application able to run on top of McU.
            - Crypto currency "wallet" application
                - e.g: Bitcoin, Bitcoin cash, Ethernum, Ripple..etc.
                - Able to install "Wallet" application that can manage and operate those specific crypto currency.
                    - Able to install, uninstall, enable, disable, stop, start the specific application.
                    - Able to execute the installed application on McU to control basic input/output interface, include and not only button, navigation sub-systems, display sub-systems.
                    - Able to control/execute secure element to proceed necessary crypto currency related operation.
            - Crypto currency support updater
                - Able to update exist "Wallet" application in place to update new specific and function added after user install wallet application.
        - Device health check
            - Able to do device health check and security check once user connect device to laptop/mobile devices.
    - Hot Wallet and Web Wallet support: Google Chrome application type hot wallet application to connect Version One to do crypto currency transaction.
        - 17shopping Wallet for Bitcoin

            - Based on Bitcoin-core (TBD, depend on engineering team decide go for native Win32 or Chrome based application)
            - Able to display current Bitcoin value on cold wallet
            - Able to display executable function(s) based on current Bitcoin value, include but not only below.
                - Value: Current value
                - Operation: transfer in (hot wallet) to single address.
                - Operation: transfer out (hot wallet) to single address.
                - Operation: confirm the transfer using cold wallet function
                - Operation: transfer from (hot wallet) to cold wallet
                - Operation: transfer from cold wallet to hot wallet
                - Operation: display remain value
                - Operation: house keeping
        - (TBD) Bitcoin Core
        - (TBD) Ethereum

<u>Version One Cold Wallet Functional specification</u>

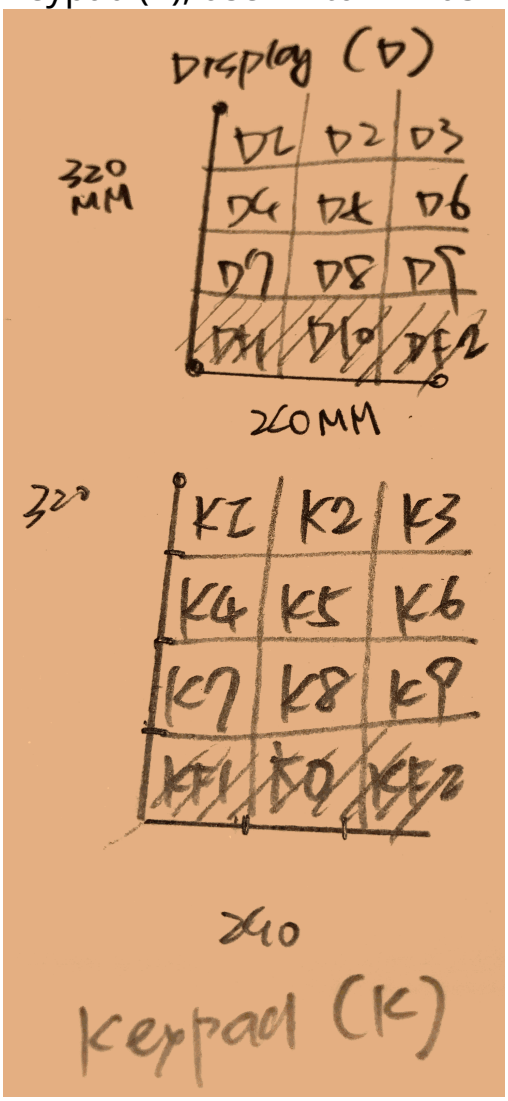
- Unbox and OOBE
    - (TBD)Unbox instruction
        - Package design (TBD)
        - User guide design (TBD)
        - Accessories and part design (TBD0
    - (TBD)Welcome screen
        - First power cycle: user first power on the device, the device first time initial, system need to run certain boot-up process to complete first boot then move to interaction mode.
        - (To be complete): Internal tracker, counter in hardware basis

        - A “Welcome screen” need to display between boot up to interaction mode.
        - Welcome screen specification
            - Power on splash screen: 17shopping logo (2-inch, Resolution TBD depend on boot time system ability), run-robin display till system go into interaction mode.
            - First initial tutorial screen: step by step interactive guide for first time use, need collect below information.
    - (TBD)EULA display
    - Create your first wallet
        - Create wallet
            - Wallet name
            - Wallet description
            - Passphrase setup
                - Setup passphrase
                - Verify passphrase
            - Advance feature
                - Passphrase setting
                    - memory usage(kB)
                    - Target compute time (MS)
            - Backup wallet
                - Printable paper backup
                    - (TBD)Preview in device
                    - Connect to printer
                - (TBD)Digital backup
                - (TBD)Export key list
    - Application Drawer UI
        - Launcher user interface show current installed/available application on device
        - Include but not limited to:
            - Wallet application for crypto currency
            - Tutorial
            - Setup
    - Wallet operation:
        - Display support crypto currency

            - Display current available crypto currency value
            - Generate receiving addresses for the wallet
                - In plain text
                - In QR code format
            - Sing translation created from online target
            - Sign transaction/message(s)
        - Advance wallet operation
            - (TBD)
        - Wallet maintains
            - Create backup of wallet
                - Route back to “Backup wallet” section
            - Change wallet encryption setting
        - System
            - Initial wallet identifies
            - Passcode/recovery code
            - Wallet function overview
            - Sign transaction
            - Backup and recovery
- Setting
    - Time and date
        - Access time/date information from laptop/mobile
    - Language
        - English
        - Spain
        - German
    - (TBD)Input support
        - Multi-key English input
    - USB setup
    - System update
    - About
        - Software license disclaimer
        - Customer support
        - Debug information

<u>UX and UI Guideline</u>

- Multi key menus based UX
    - Physical keypad

    - Display (D), use D1 to D12 represent application icon and function area
    - Keypad (K), use K1 to K12 as keypad position
    - 

- Refer to separate document for UX flow and design