CRAYONIC

SECURE DIGITAL IDENTITY

Crayonic KeyVault™
Technical and Security Whitepaper

Version 0.9, 2/2021

CONTENTS

Introduction

Crayonic KeyVault™ is a smart authentication hardware device for securing digital transactions in online and offline environments. Crayonic KeyVault™ enables highly secure identification and authentication of its owner for many use cases. It uses multiple standards and well-defined protocols.

Crayonic KeyVault™ is a FIDO2-compliant security key providing superior resistance to phishing, man-in-the-middle attacks, credential stuffing, and keyloggers.

It uses a combination of machine learning and cryptography to guarantee, with the highest confidence, the real identity of a person performing authentication and even their willingness to transact – all without disclosing any sensitive details about the person.

The KeyVault secures all personal sensitive information such as biometric templates, cryptographic keys, credentials, X509 certificates, etc. It allows the owner of the device to securely use this data to interact with other devices and applications.

Identification and authentication of the user are based on multiple knowledge and biometric factors, thus meeting the triple factor authentication criteria for high security use cases. It combines static biometrics, such as a person's fingerprint and behavioural biometrics, with dynamic characteristics such as the user's handwriting and/or voice.

The level of user authentication can be adjusted according to the pre-set security policy or stepped-up by the relying party per transaction from a simple button press to multiple biometric and knowledge challenges.

Some of the core features of Crayonic KeyVault™ include:

- Passwordless and even usernameless authentication using the FIDO standard over USB, BTLE, and NFC communication channels.
- Smart card emulation using PIV and PGP standards using NFC (ISO14400) and USB (ISO7816) communication.
- Support for e-signature utilizing eIDAS Qualified Certificates over FIDO or PIV protocol.
- Legacy one-time password support (TOTP, HOTP) using secure display.
- AES encrypted mass storage (up to 128MB FAT16/32) for highly sensitive documents.
- Generic key/value store for securing legacy shared secrets such as passwords.
- Support for offline signing of blockchain transactions (Ethereum and Bitcoin compatible with plans to support Cardano and other blockchain projects).
- Rugged and waterproof casing with sealed electronics for maximum physical security.
- Developed, manufactured, and assembled by Crayonic in the European Union.

Architecture

The entire solution consists of hardware and software layers. The architecture describes the logical and physical structure of the product.

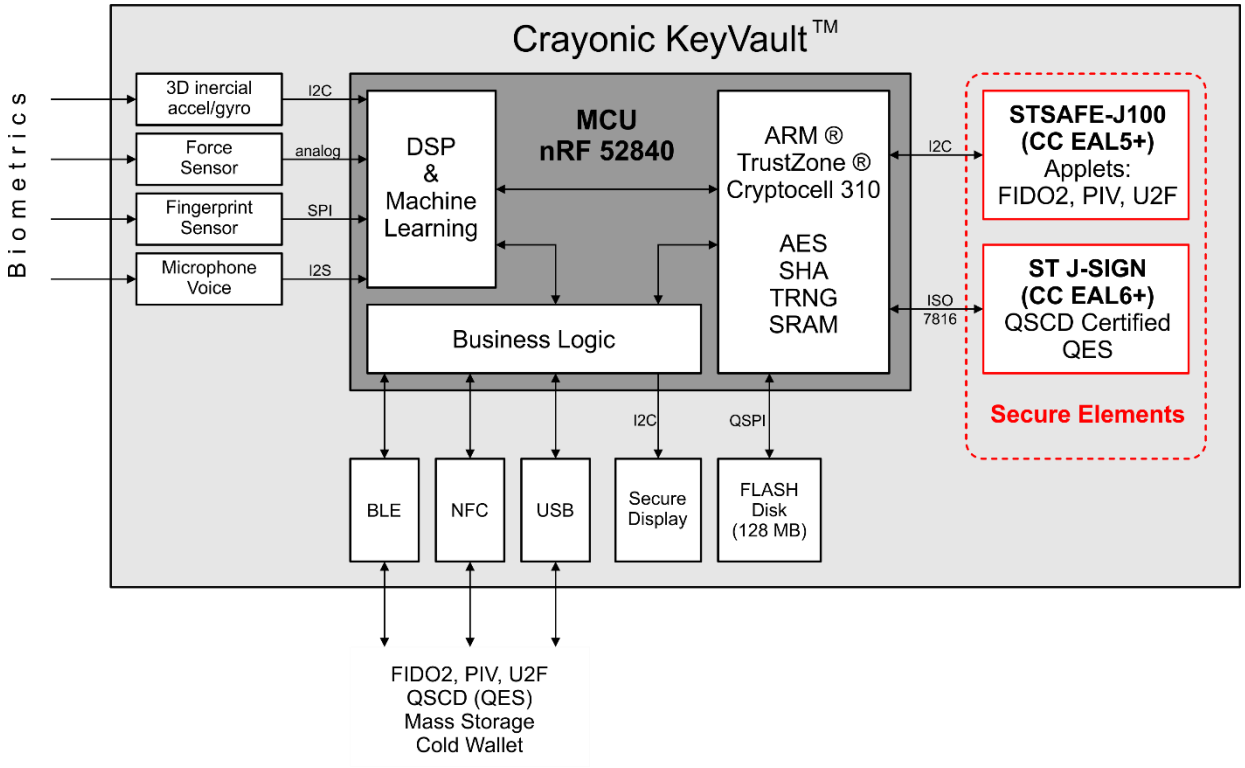


Image 1: Solution architecture

The KeyVault is based on architecture that leverages two core processing units:

1. Generic Microcontroller Unit (MCU).
2. Secure Element (SE).

The MCU supports all supporting operations related to secure services provided by the KeyVault:

- Communication with host application via USB, NFC, or BLE.
- Communication with SE.
- Communication with biometric sensors.
- Biometric data processing.

The SE is Common Criteria (CC) EAL 5+ certified and ensures all sensitive operations, e.g.:

- Random seed and key generation.
- Key derivation.
- Key storage.
- Signing and encryption transactions.
- Communication with the MCU.

Biometric sensors include:

- Fingerprint scanner.
- Accelerometer/Gyroscope and force sensor for handwriting input and recognition.
- Microphone for optional voice input and biometric recognition.

Other important hardware components include:

- OLED graphics display for transaction confirmations and KeyVault settings.
- NAND flash memory for encrypted mass storage.
- LiPo 70 mAh rechargeable battery for enabling Bluetooth communication and standalone authentication (100 mAh in the next release).
- Micro USB connector for USB connectivity and battery charging.

The Crayonic KeyVault™ casing has been designed to physically protect electronic components against disassembly, side channel attacks using electromagnetic waves, and accidental destruction.

Operational Environment

Crayonic KeyVault™ is an independent, self-standing tool, requiring no central control system. It is, therefore, an autonomous solution supporting various scenarios and interoperability using state-of-the-art protocols and connection interfaces.

The KeyVault is used as a personal device, not shared with others. Hence, each user gets their own device and personalizes it by training it to their biometrics, knowledge, and behaviour.

It is possible to initialize a new factory delivered device or erase and re-initialize previously used devices. Optionally, in case of stolen, lost, or broken device it is possible to use backed-up master entropy to create a new digital copy of the original device utilizing a secure Shamir Shared Secret scheme in combination with AES encrypted metadata backup.

The KeyVault use cases depend on applications it interacts with. The connection options include Bluetooth low energy (BLE) and near-field communication (NFC), as well as wired USB to connect with other devices like mobile phones and laptops.

Any operation on key material stored in KeyVault's Secure Element (SE) is confirmed using information visible on a Secure Display. Depending on the operation required by an app or remote service on the connected device, a user may be asked to perform actions to provide their biometry-authenticated identity or to authorize the operation itself. The identification and authorization are based on the user's biometrics and/or secret knowledge (PIN or passphrase). Positive identification allows access to operations using the sensitive data (keys) for common cryptographic operation (e.g., digital signature, encryption, and decryption).

The device provides secure communication with external applications, interaction with a user, and at the same time protects the sensitive data stored in the SE. The user's private keys, protected by the SE, never leave the secure certified storage of the device. The master entropy from which all key material is derived is split into multiple Shamir shared secrets and optionally available for backup to the user/administrator via multiple trusted service providers (certified TSPs) with the capability to store keys in custody.

Only after a rigorous KYC process are the Shamir secrets released to a trusted KeyVault device for possible entropy recovery. After the required quorum of parts has been recovered within the new KeyVault device, the master entropy is finally calculated and used to derive backup AES-256 encryption key. The backup encryption key is then used to recover metadata from an encrypted backup that can be made available on cloud servers such as Crayonic Gateway™. The process of metadata backup recovery is transparent to end-users as it utilizes FIDO protocol to store and get this metadata.

Assumptions

The KeyVault security model assumes that a user follows certain security rules:

1. The PIN should be kept secret even if it's protected by a user's own handwriting/voice.
2. Recovery secrets must be kept secret across multiple trusted parties.
3. All personalization operations should be done within a private environment.
4. All transaction details must be verified on the secure display and only then confirmed valid by the user to prevent the most sophisticated types of man-in-the-middle attacks.

Features and Use Cases

Crayonic KeyVault™ use case summary:

- FIDO U2F/UAF and FIDO2 security key over USB, BTLE, and NFC channels
- PIV and PGP smart card emulation over USB and NFC channels
- OTP authentication (OATH TOTP, HOTP standards)
- Blockchain transactions authentication (i.e., Ethereum/Bitcoin signing standards)
- Advanced and Qualified Electronic Signature according to ETSI TS 119 312
- Secure mass storage (USB with FAT32 support)
- Secure key/value storage over FIDO2 protocol (i.e., for legacy password managers)

Security Key for FIDO2 authentication

Crayonic KeyVault™ supports

- legacy FIDO Universal Second Factor (U2F)
- as well as the latest FIDO2, including Client to Authenticator Protocol - CTAP2 required for W3C Web Authentication - WebAuthn.

It can be used to securely access online services with two-factor, multi-factor, or even passwordless authentication. In this concept, a password that a user needs to remember is replaced by a key pair stored in the Crayonic KeyVault™.

Sensitive cryptographic operations required for FIDO2 authentication are offloaded to KeyVault – a roaming biometric hardware authenticator that can be accessed via USB, BLE, or NFC. The primary KeyVault use case is for the initial authentication on a new client device, on devices that are rarely used or don't include a platform authenticator, or when it is required to keep the authenticator separated from the clients it is used with.

Thanks to KeyVault's architecture and several security improvements in the software and hardware, including the usage of Common Criteria certified Secure Element, the KeyVault device meets requirements for FIDO Certification Level 3. Currently, Level 1 certification has been issued due to the lengthy security audit processes. For clients requiring the highest level of certification, Crayonic can offer its full participation in a custom security audit process. The Biometric Component Certification and Authenticator certification process for the KeyVault are in progress.

FIDO2 / WebAuthn

When compared to its predecessor, FIDO U2F, the FIDO2/WebAuthn authentication enables complete passwordless multi-factor authentication with login credentials unique across all relying parties, thus supporting maximum user privacy. User's biometric data never leaves the KeyVault authenticator. The user verification is done locally, on the device, and secret and biometric information stored on the KeyVault are never shared with the service requiring authentication.

The WebAuthn specification defines 3 roles:

- WebAuthn Relying Party – a website or service requiring authentication.
- WebAuthn Client – a browser on a user's device.
- Authenticator compatible with the WebAuthn Client – the KeyVault device.

Registration Process

1. During the registration process, WebAuthn Client sends the Relying Party ID and info, user info, and Client data hash value.
2. The user authenticates into the Authenticator (KeyVault) using the requested combination of PIN and biometrics.
3. The Authenticator (KeyVault) creates a new asymmetric key pair, storing the private key in the SE for later.
4. The Authenticator (KeyVault) then signs an attestation statement with an attestation private key stored in the device during the manufacturing process.

   Signing the attestation statement proves the authenticity of the device and guarantees that user credentials are bound to the Crayonic KeyVault™ authenticator. The attestation statement includes metadata with an Authenticator description. It also includes a new user public key checked by the Relying Party during the authentication process to verify the signed authentication assertion.

Authentication Process

1. During the authentication process the WebAuthn Relying Party sends a challenge with authentication metadata to the WebAuthn Client.
2. The WebAuthn Client sends the Relying Party ID and Client data hash value to the Authenticator (KeyVault).
3. The obtained data together with Authenticator data is then sent back as a signed assertion after proper user verification (PIN, biometrics) by the KeyVault. The locally stored roaming credentials, including the proper private signing key, are identified by the relying party ID. The signature of the assertion can be verified by the relying party using the user's public key obtained during the registration process described above.

   #### Username-less Authentication

   FIDO2 also allows for so-called *resident keys* and their discovery by the remote Relying Party. This feature allows even for the user name to be removed from the passwordless authentication:

   - If only one credential is stored per the Relying Party it will be automatically selected and sent with the signed challenge. This enables a very fast multifactor authentication especially if the user is pre-authenticated within the KeyVault. (Pre-authentication is not a standard FIDO2 feature but may be allowed for a custom time period by the administrator on the Crayonic KeyVault™).
   - If multiple account keys are stored on the KeyVault authenticator (i.e., Relying Party credentials), the user simply selects from the stored keys by scrolling through the KeyVault's display. Thus, allowing selection of the correct user for the site.

During an authentication or transaction confirmation event, the Crayonic KeyVault™ verifies the user who needs to present their biometric data and then unlocks the *AppID* specific private key. The private key is then used to sign transaction data and send it to the Relying Party.

The KeyVault also allows a de-registration from a previously registered Relying Party. In such case, all related *AppID* key data are deleted from KeyVault's internal storage.

FIDO U2F (backward compatible legacy feature)

The FIDO U2F authentication scheme supports only the second-factor experience. It allows adding a strong second factor to the existing password flow. The online service can prompt the user to present the KeyVault (FIDO security key, U2F token) at any time by simply connecting the device via USB and pressing a button or tapping over NFC or BLE. The KeyVault then uses a private key, part of asymmetric key pair generated and handled by the SE, to log in. Key pairs are unique for each tuple of the relying party, user account, and KeyVault device.

During the initialization process of the token two random values are generated by the Secure Element RNG: a *seed* and a *secret key* for MAC computation. Both values are stored in the KeyVault and never leave it. Users may initiate a reset of the values, then the *seed* and *secret key* will be deleted, and new values are generated in a new initialization process. The token also includes externally generated attestation key pair and certificate serving as a trust anchor for the authenticity of the authenticator.

During each registration process, a new unique asymmetric key pair is generated based on the AppID of the relying party; a random nonce is generated by token, as well as the KeyVault's seed. To generate a key handle used later during the authentication process to recover the generated key pair, the token computes MAC over the AppID and a nonce using the secret key. The private key from the key pair is generated temporarily on the authenticator and never leaves the KeyVault.

During authentication, the KeyVault obtains the AppID, a challenge and previously registered key handle. The token verifies the MAC and re-generates the private key using the stored seed, which is then used to sign the AppID and challenge. After successful verification of the signature with the public key of the authenticator, previously stored by the relying party during the registration process, the relying party can accept the user authentication to the service.

PIV and PGP smart card emulation

Crayonic KeyVault™ supports emulation of smart cards over ISO standards using NFC and USB communication channels. Both PIV and PGP (in the upcoming KV version) are implemented as independent applets residing in the Secure Element. They are initialized during manufacturing and accessed by PIN code entered on the KeyVault itself utilizing secure PIN input. Optionally, a PIN can be mapped to a registered fingerprint thus enabling the biometric authentication to smart card feature. PIV applet follows NIST SP 800-73-4 standard and thus is compatible with Windows, Linux (OpenSC), and MacOS operating systems.

PIV applet supports:
RSA 1024/2048 keys, EC P-256/384 keys, EC Diffie-Hellman, ECDSA and AES for admin keys.
The PIV applet can be managed by Crayonic PIV Management tool on Windows clients and also remotely by Crayonic Gateway™ over FIDO2 protocol using custom Crayonic extensions.

NOTE: PIN code sent by external device to KeyVault will be overwritten by KeyVault PIN entry system.

KeyVault supports issuing of X509 certificates into the KeyVault using offline tools or remotely using custom FIDO2 extensions. This allows for easy management of certificates even in PKI infrastructure with the ability for end users to self-service the issuance and re-issuance.

Biometric Handwritten Electronic Signature

Crayonic KeyVault™ provides functionalities for creating secure electronic signatures and in combination with external applications; it complies with requirements for eIDAS PAdES compliance.

While the e-signing application handles operations on a document to be signed, the KeyVault device provides all operations for the signature creation secured by handwriting biometrics.

During the handwritten signature operation, the sensors capture unique dynamic characteristics of the user's movement (position, velocity, acceleration, pressure, and air moves). The hash value of biometric data is combined with the document content and added to the document metadata. The original biometric data can be encrypted with a pre-defined key and optionally used to analyze the handwritten signature by a forensic expert.

The application should calculate a hash value from the document content, encrypted biometric data, and other metadata. The KeyVault user should compare the hash value provided by the application with the hash value visible on KeyVault Secure Display, which both have to be identical. To create the actual digital signature the application creates a one-time key pair unique for every signature, and after applying it to the document the private key is discarded. There is no requirement for biometric handwritten signature to have a pre-issued X509 certificate and thus could be executed by anyone holding the KeyVault.

E-Signature using TSP issued X509 certificate.

The act of electronic signature (creating the signature using a private key) may require the input of the user's secret information (PIN code), which identifies and authorizes a particular private key holder. The KeyVault provides the ability to use biometric sensors and stored biometric characteristics of the user for user authentication in addition to the PIN code when it is entered using the biometric sensors.

Qualified Electronic Signature as per eIDAS can be created using pre-generated private keys with a TSP signed X509 certificate. This certificate is used in place of the biometric handwritten signature as described above. The QES certificate issued for the owner of the KeyVault, which can act as a Secure Signature Creation Device, is signed by a Trust Service Provider after the know-your-customer (KYC) procedure. KeyVault is certified to store such high level of assurance identity certificates assuming the correct integration with the TSP certificate authority.

After entering the PIN code using voice or handwriting the KeyVault can unlock a digital signing certificates over the PIV smart card standard or even over FIDO2 protocol for easy integration.

Blockchain support

The Crayonic KeyVault™ provides hardware wallet offline signing service for processing transactions on crypto-assets i.e., to receive and perform payments in cryptocurrencies.
The KeyVault handles secure cold storage for private keys, allowing users to store their private blockchain keys locally, on their own device. The private keys stored in the SE never leave it and are only used for operations confirmed by the user's authentication and shown in the secure display.

In cases when a user's device is lost, damaged or when the user simply wants to move the wallet to a different device it is possible to restore the set of wallet private keys with a *recovery seed*. This is supported by the implementation of a hierarchical deterministic (HD) wallet (BIP-0032) with a one-time backup.

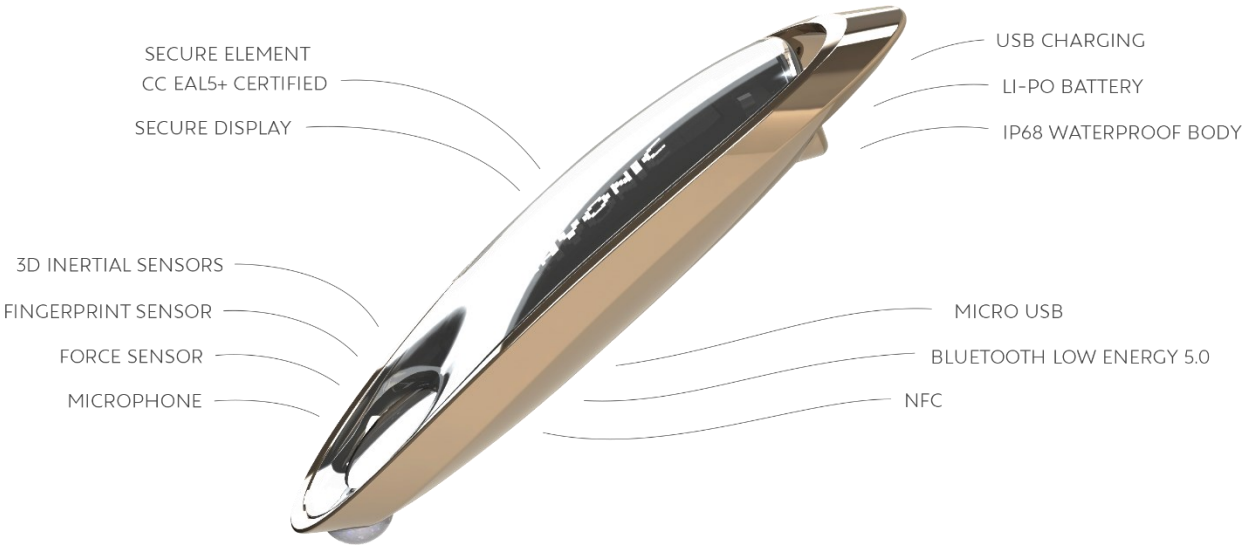
A single *recovery seed* created during the initialization of the wallet can be backed up and stored offline. On the other hand, whoever gets access to the recovery seed is able to generate the entire tree of children key pairs, therefore it should be properly safeguarded. It is suggested to encrypt the *recovery seed* and/or use KeyVault's secret sharing mechanisms, i.e. a Shamir Shared Secret (e.g. SLIP-0039) and store the shares in different trusted parties secure stores.

The logical hierarchy of the implemented wallet is defined by BIP-0044 and allows handling of multiple cryptocurrencies (coins), accounts and external/internal chains per account.

The Crayonic KeyVault™ will initially support Bitcoin and Ethereum signatures with future support for Cardano (ADA) transaction signing. Cardano blockchain may be used in the near future as a HW wallet attestation anchor to help prove authenticity of the wallet by recording its DID on the chain during manufacturing.

Hardware Design

Crayonic KeyVault™ has been designed with multiple use cases in mind, which is reflected in its unique shape. The simple use case of authentication is enabled by either pressing a button at the front bottom or touching a fingerprint reader on top. For use in handwriting scenarios, i.e., handwritten PIN entry, the device can be held like a pen for writing on a smooth flat surface such as mobile device screen or table top. For handwritten signatures executed on mobile devices, the rubber button serves as the tip of the pressure sensitive stylus – compatible with most touch screens.



Casing

Dimensions: 74 mm x 24 mm x 13 mm
Body: Easy to clean and disinfect metal & plexiglass (IP68 waterproof in the next release)
Battery: Lithium-Polymer with 70 mAh capacity (100 mAh in the next release)
Display: 128 x 32 pixels OLED graphics display
Charging: Micro USB port (USB-C in the next release)

Components

Microcontroller Unit (MCU)

In the first version of KeyVault, we utilize the nRF52840 System on Chip from Nordic semiconductor built around the 32-bit ARM® Cortex™- M4 CPU with floating point unit, running at 64 MHz and with on-chip ARM® CryptoCell cryptographic accelerator. It has numerous digital peripherals and interfaces.

Secure Element

The Secure Element (SE) covers all crucial operations during the lifetime of sensitive private data and allows the physical separation of these data from the rest of the system. For this purpose, we use ST's STSAFE-J chip. The device embeds a secure Java Card operating system compliant with GlobalPlatform.

The chip's key features supporting KeyVault security are:

- ECC support
- ECDSA digital signature generation and verification
- On-chip key generation
- Key agreement protocols support (ECKA-ECDH, ECKA-EG)
- Key pair, public key and PIN objects
- TRNG
- Cryptographic algorithms support (ECC, AES, SHA)
- DPA and DFA countermeasures against side-channel attacks
- Common Criteria certification EAL5+

The SE protects following operations in the KeyVault:

- Secure keys storage
- Secure cryptographic operations on keys (encryption, signature…)
- Secure communication with devices and applications

Software Design

Firmware

There are two types of firmware running inside the KeyVault:

1. Firmware running on top of MCU (nRF52840)
2. Firmware running on top of SE (STSAFE-J)

MCU Firmware

The KeyVault main control unit covers the following function areas:

- Data processing of the biometric data provided by the connected biometric sensors (fingerprint, voice, force, 3D inertial motion…)
- Cryptographic operations acceleration and secure connection to the SE.
- Data communication with remote applications via wired and wireless interfaces (BLE, NFC, USB) and visual communication with a device user via the secure graphical display.

The MCU also includes business logic supporting a proper functionality for the main services of the KeyVault: a signature creation device, FIDO authenticator, and crypto HW wallet. The security of the services depends on proper HW design and architecture as well as software implementation.

Secure Element Firmware

The SE firmware is in charge of:

- Communication with external elements.
- Performing cryptographic operations (encryption, digital signature, random number generation, key derivation, Shamir Secret store, etc.).
- Storing secret data (PIN, seed, private key).
- Providing a set of functions via API (communication, cryptography…).

Communication with Client Application Using Bluetooth Low Energy

Secure communication between the KeyVault client application device (laptop or smartphone) requires pairing. It involves authentication of the device identity, encryption of the link using a short-term key (STK), and distribution of the long-term encryption keys (LTK).

The BLE encryption is based on the 128-bit AES-CCM standard, LTK is used to create the shared secret key. We require the clients to be paired with KeyVault to support:

- Security Mode 1
- Security Level 3 (authenticated pairing with AES-CCM encryption)
- or Level 4 (Authenticated LE Secure Connections pairing with AES-CCM encryption using ECDH for LTK generation, 4.2 devices only).

During the pairing procedure we apply the authentication methods that provide protection against the man-in-the-middle attacks:

- Numeric comparison (only for 4.2 devices, with LE Secure Connections) – starts as just works pairing method – devices exchange their public keys, generate a nonce, use it to generate a confirmation value, and send to the other party. Once the match is confirmed, both devices generate a 6-digit confirmation value using the nonces and display the values to the user who manually checks the matching of both values.
- Out of the band – another wireless channel (NFC) is used to transfer additional data assisting the pairing procedure (assumes the security of NFC connection).

Authorization

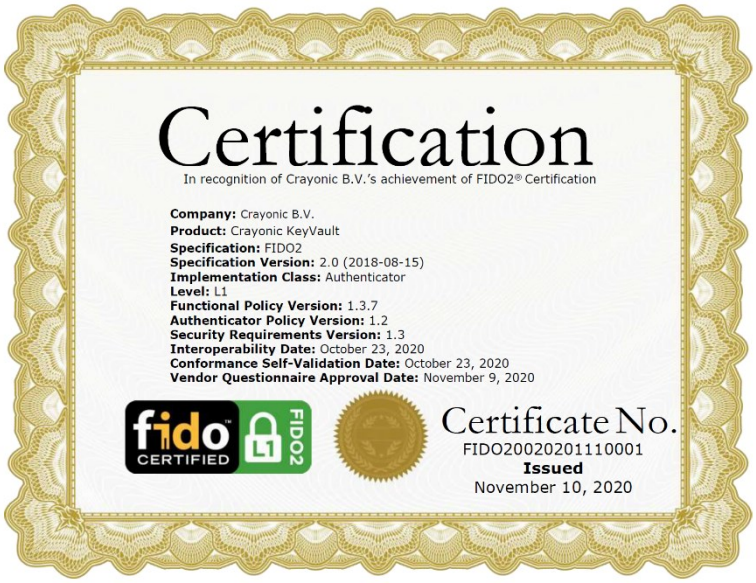
PIN

PIN code stored in the SE can be used for any authorization scheme requiring something that the user knows. The KeyVault provides an option to enter the PIN in handwritten or voice form. The PIN is then recognized by the machine learning code running on the MCU and is compared within SE with the stored value.

Biometrics

KeyVault features powerful biometric sensors for identification and authorization of the user and thus allows passwordless, user-friendly, scenarios. Fingerprint machine learning algorithms are used at the basic level of biometric authentication. To step-up the security and assurance level of identity of the KeyVault owner, additional behavioural biometrics may be requested by the relying party. The behavioural biometrics is possible if the user has trained digit entry using either handwriting and/or voice (if handwriting/voice are enabled by the KV security policy).

As a result, there are no trade-offs needed between the password/PIN memorability and its length or complexity. Instead, we use state-of-the-art cryptographic algorithms and brute force resistant length for keys. The operations on securely stored private keys are possible only after a positive authentication of the user, using one or more biometric methods available in KeyVault.



Device Initialization

There are two types of device initialization – factory initialization and user initialization (personalization). While the factory initialization is done only once during the device lifetime, in a protected factory environment allowing proper security settings of the device, the user initialization can be done each time a new user starts to use the device.

Factory Initialization

During the factory initialization, we create foundations for secure communication between the elements within the device (between the MCU and SE) as well as between the KeyVault and other devices by creating authentication credentials. The secure channel between the MCU and SE is created during manufacturing after final testing of the hardware by executing standard DH key exchange between the SE and MCU.

The symmetric AES encryption key is created only once and stored in SE for its lifetime and in MCU ACL protected flash using the following strategy:

1. Store the key in a reserved flash region.
2. Enable read-back protection using a Control access port. This prevents a debugger from accessing the flash (the only way to disable it is to first do a full chip erase).
3. In the bootloader:
    a. Read the key from flash and copy it to CryptoCell (secure always on RAM).
    b. Enable ACL to protect the key so that it cannot be accessed by the application. This protects the key against most attacks (excl. decapping).

Next, an asymmetric key pair is created, with a private key stored in the SE, and a public key certificate signed with Crayonic CA. These authentication credentials can be used to verify the authenticity of the KeyVault device by other services. The Crayonic root CA certificate is also stored securely to each device in order to provide a trust anchor for authentication of the services by the KeyVault.

User Initialization

The initialization (re)creates all internal data structures required for the proper functioning of the device. There is an option to recreate a part of the KeyVault's data structure based on the user's master seed and, in this way, create a logical copy of the original device used for master seed generation. This option is especially useful in cases when the original device was stolen or broken, and we want to allow a user to move to another device smoothly.

During the user initialization process, new master entropy is generated in the case of a new user, or provided by a user as an input for the derivation of the key structure previously generated in another KeyVault device.

1. Master entropy (seed) generation
    a. There are two structures of key pairs we allow users to recreate from a seed value - FIDO authenticator keys and hardware crypto wallet keys (hierarchical deterministic wallet).
    b. We use the SE's certified True Random Number Generator to generate random values for master entropy. Based on the seed, the whole key tree of the keys can be derived following the wallet hierarchy according to BIP-0044. Similarly, the key pairs for the FIDO authenticator can be derived from the master seed using a key derivation function from the FIDO Authenticator Allowed Cryptography List.
    c. Possessing the master seed allows anybody to create a logical copy of the wallet or authenticator on a different device.
    d. To improve the level of protection for the master seed the KeyVault supports the Shamir Secret Sharing (SSS) algorithm. The algorithm splits the master seed into unique parts that can be distributed among participants. In order to reconstruct the original secret, a specified minimum number of parts are required to be supplied. The SSS implementation follows the SLIP-0039 standard. The master entropy is split into multiple Shamir Shared Secrets and stored in the SE for later possible export to trusted third party stores. Trusted third party seed backup stores need to prove their identity to the KeyVault using X509 signed certificate, which evaluates to the trusted Crayonic Root certificate. Only after proving the remote service identity, the entropy part (one of N secrets) is exported from KeyVault to the remote service as part of multiparty computing scheme entropy backup.

2. Hardware wallet private keys generation based on the master seed
    The hierarchical deterministic wallets based on BIP-0032 have a defined structure of wallets/accounts, chains, and addresses. The starting point to generate the wallet hierarchy tree is either an internally randomly generated master seed or a backed-up seed sequence provided as user input. The subsequent elements are generated using the Child Key Derivation (CKD) Function as defined by the BIP standard.

3. FIDO Authenticator private key generation based on the master seed
    Based on the master seed and authenticator meta-data we allow the ability to recreate a key structure for a FIDO authenticator. A key derivation function from the FIDO Authenticator Allowed Cryptography List is applied to derive the keys. The meta-data with non-sensitive information on services, for which the Authenticator was used, can be stored separately.

4. Biometric characteristics initial training
    Before starting using the KeyVault's biometric features for user identification and authorization, the user needs to create a personalized biometric profile. The hosted application will ask users to perform various actions – say a few words, handwrite a few symbols or digits, based on which a tailored biometric user profile is created and stored in the SE.

Conclusion

Crayonic KeyVault™ is developed, manufactured, and assembled by Crayonic in the European Union. That means you don't have to worry about an insecure supply chain.

The KeyVault is backward compatible with legacy systems such as FIDO U2F, TOTP, and HOTP. It is waterproof and has unique biometric features unavailable in other products.

It supports up to 128MB of AES encrypted mass storage as well as the ability to sign blockchain transactions offline.

It complies with all necessary industry standards and the tamper-proof Secure Element (SE) allows for physical separation of sensitive private key data.

With our unique, though optional, KYC-enabled recoverability solution, keys are securely split into multiple parts, encrypted, and securely stored with the parties of your choice.

The Crayonic KeyVault™ offers all of the modern, and necessary, features to help transition your organization to a truly secure, and passwordless, future.

References

1. CTAP
2. WebAuthn
3. Biometric Component Certification
4. Authenticator certification process
5. BIP-0032
6. BIP-0044
7. SLIP-0039
8. FIDO Authenticator Allowed Cryptography List