Product Description

The OFFPAD and OFFPAD+ are FIDO2 security keys leveraging fingerprint biometrics to optimize the balance between security and convenience.

FIDO2 is a global and standardized authentication process supported by major industry players such as Google, Microsoft, Apple, and Samsung, offering the gold standard of authentication.

FIDO2 replaces password-based authentication and traditional Multi-Factor Authentication (MFA) with public key cryptography. FIDO2 enables users to leverage common devices to easily authenticate to online services in both mobile and desktop environments.

PONE Biometrics takes your privacy seriously. Your biometrics are encrypted and stored securely on the FIDO2 security key. Your biometrics are never shared outside the device. As a user, you own your biometrics.

The OFFPAD and OFFPAD+ embeds a long-lifetime battery. Your device is always ready to be used and can be quickly recharged with a simple wireless charger. Through the card holder the OFFPAD+ also enables charging through a USB cable.

Features

The features supported by the OFFPAD is defined in the FIDO2 specification.
The FIDO2 specification is a set of standards for strong authentication developed by the FIDO Alliance (Fast IDentity Online) and the World Wide Web Consortium (W3C). FIDO2 aims to enable secure, passwordless authentication and is a more advanced version of the original FIDO (Fast Identity Online) standards.

More details about the features supported by OFFPAD and OFFPAD+ can be found in the Feature Guide.

Connectivity

The OFFPAD communicates with devices by using Near Field Communication (NFC) or Bluetooth Low Energy (BLE). In addition the OFFPAD+ enables USB connectivity through the specially designed card holder. More information on how to connect the OFFPAD and OFFPAD+ to a device can be found in the Usage Guide.

Biometrics

The OFFPAD and OFFPAD+ is built with a fingerprint biometrics sensor to deliver an optimal user experience. The off-chip capacitive sensor separates the fingerprint sensing elements from the chip that acquires the image and processes the biometric data. This ingenious design ensures excellent security, significantly higher image fidelity, superb noise immunity, and market-leading usability under real-world conditions. This sensor is bendable and durable facilitating a long life of the device. Thanks to ultra-low power consumption, battery life is optimized. The superior level of security and excellent image fidelity provides outstanding biometrics and user performance.

Display

The OFFPAD and OFFPAD+ has an E Ink display, short for electronic ink, a type of screen technology designed to mimic the appearance of ink on paper. Unlike traditional LCD or OLED screens, E Ink displays don't emit light directly. Instead, they use tiny capsules filled with charged black and white particles that move when an electric field is applied, creating text and images on the screen.

The E Ink display has been added to improve the customer experience. You always know what you are authenticating to and you can follow the fingerprint enrolment steps in a convenient way.

Battery

To provide you with the best autonomy possible, there is a battery embedded in our FIDO2 Security keys. The Li-ion rechargeable battery specially designed to offer high heat resistance, safety (high reliability), high output, and long lifetime.

The battery is charged using the open interface standard defining wireless power transfer via inductive charging: Qi. This standard has been developed by the Wireless Power Consortium and is supported by all electronic device manufacturers such as Apple, Asus, Google, Huawei, Samsung, Xiaomi, and Sony. Any charging pad supporting Qi can be used.

The OFFPAD+ also supports charging through a USB cable.

Feature Guide

FIDO2 comprises two main components: WebAuthn (Web Authentication) and CTAP (Client To Authenticator Protocol).

WebAuthn is a web standard developed by W3C, which provides a way for web applications to integrate strong, passwordless authentication using public key cryptography.
WebAuthn allows browsers and servers to interact with external authenticators (like the OFFPAD or OFFPAD+) to verify the user's identity.

CTAP is a protocol developed by the FIDO Alliance that enables communication between a device (e.g., a phone or computer) and an external authenticator (e.g., a FIDO2 security key, a biometric sensor, or a smartphone app).
CTAP allows devices to work together to authenticate users, such as using a phone as an authenticator or a hardware token (like the OFFPAD or OFFPAD+) to perform the authentication process.

FIDO2 Make Credential

FIDO2 Make credential is used to create a new credential (also known as passkey) that is bound to:

- The relying party (website or service).
- The user's security key (e.g. OFFPAD or OFFPAD+).
- The user verification method (if required, like PIN or biometrics).

The steps for FIDO2 Make Credential are:

1. Client Sends a Registration Request
    - The website or service (Relying Party, RP) asks the user to register a security key.
    - The browser (or OS) forwards this request to the security key.
2. Authenticator Generates a Key Pair
    - The security key generates a new public-private key pair.
    - The private key stays on the security key, while the public key is sent back to the RP.
3. Attestation & User Verification (if required)
    - The authenticator may require user verification (UV) via PIN or biometrics before completing the process.
    - The security key signs the public key with an attestation certificate, proving it was generated securely on a valid device.
4. Client Sends Credential to the Relying Party
    - The browser/OS sends the new credential (public key + attestation) back to the website.
    - The RP stores the public key and associates it with the user's account.

Credential is Now Ready for Authentication!

Next time the user logs in, their FIDO2 key can use this credential to prove their identity via FIDO2 Get Assertion.

FIDO2 Get Assertion

FIDO2 Get Assertion is used during the authentication phase of a FIDO2-based login. It enables a user to authenticate themselves securely to a relying party (website or service) using a previously registered credential (see FIDO2 Make Credential), without relying on passwords.

Steps for FIDO2 Get Assertion (Authentication Process) are:

1. Client Sends an Authentication Request
    - The website or service (Relying Party, RP) asks the user to log in with their FIDO2 security key.
    - The browser (or OS) forwards this authentication request to the security key.
2. Authenticator Finds a Matching Credential
    - The security key checks if it has a credential linked to the RP ID.
    - If multiple credentials exist, the user may need to select one.
    - If no credentials match, authentication fails.
3. User Verification & Assertion Signing
    - If required, the authenticator asks for user verification (UV) (e.g., fingerprint, PIN, or touch).
    - The security key then:
        - Uses the private key to sign the challenge.
        - Includes additional security data, such as a counter to prevent replay attacks.
4. Client Sends Assertion to the Relying Party
    - The browser/OS sends the signed assertion back to the website.
    - The RP verifies the signature using the stored public key.
    - If the signature is valid, the user is authenticated successfully.

FIDO2 Client PIN

FIDO2 Client PIN is used to manage PIN-based user verification for security keys or authenticators. It allows users to:

- Set a new PIN (for devices that support PIN authentication).
- Change an existing PIN (if the user knows the current one).
- Verify a PIN before performing sensitive operations.

When you first register a FIDO2 authenticator (e.g., OFFPAD or OFFPAD+), the service you're using may require you to set a PIN for the authenticator. This PIN is used as a second factor of authentication, ensuring that even if someone physically steals your device authenticator, they cannot use it without the PIN. The authenticators from PONE Biometrics also support the use of fingerprints as a second

factor.
How to set the PIN and add fingerprints is described in the getting started guide.

The PIN and fingerprints are stored securely on the authenticator. They are used to unlock the device and prove your identity, but the PIN or fingerprints are never shared with the service or application you're logging into. Instead, the authenticator uses the PIN or fingerprints to unlock itself and generate a secure cryptographic key, which is then used to authenticate you.

FIDO2 Bio Enrollment

FIDO2 Bio Enrollment manages biometric enrollment on authenticators that support built-in biometrics (e.g., fingerprint scanners on security keys or biometric-enabled devices).

It allows users to:

- Enroll new biometric templates (e.g., add a fingerprint).
- Remove biometric templates (e.g., delete a fingerprint).
- List enrolled biometrics (e.g., check registered fingerprints).

How to do FIDO2 Bio Enrollment on OFFPAD and OFFPAD+ is described in the getting started guide.

FIDO2 Large Blob

FIDO2 Large Blob allows FIDO2 authenticators (such as security keys) to store and retrieve arbitrary data securely. This is useful for applications that need to persist small pieces of data directly on the authenticator.

Key features:

- Secure Storage – Data is encrypted and stored on the authenticator.
- Per-Relying Party Access – Each website (Relying Parties) can store and retrieve its own data.
- Read/Write Support – Relying Parties can write, update, or read the stored data.
- Persistent Across Sessions – Unlike credential IDs, this data remains available even after multiple authentications.

The steps for FIDO2 Large Blob are:

1. Client Requests to Write or Read Large Blob Data
    - A website (Relying Party, RP) asks the browser (client) to interact with a FIDO2 authenticator to store or retrieve data.
    - The client forwards the request using the CTAP2.1 command.
2. Authenticator Processes the Large Blob Request
    - If writing data: The authenticator encrypts and stores the large blob securely.

    - If reading data: The authenticator decrypts and returns the stored large blob.
3. Client Sends Data to the Relying Party
    - The browser sends back the retrieved data (if reading).
    - If writing, the browser confirms the operation was successful.

FIDO2 Credential Blob

FIDO2 Credential Blob (Cred Blob) allows a FIDO2 authenticator (e.g., security key or built-in biometric authenticator) to store a small piece of data (up to 32 bytes) attached to a specific credential.
The Cred Blob is an optional data field stored inside a credential when it is created using FIDO2 Make Credential.
It can be retrieved later when authenticating with FIDO2 Get Assertion.

Key features:

- Credential-Specific Storage – Each cred blob is tied to a single passkey (credential).
- Up to 32 Bytes – Enough for small metadata like flags, IDs, or labels.
- Can Be Written and Read Later – Helps with credential management.
- RP-Controlled Data – The Relying Party (RP) defines the data contents.

The steps for FIDO2 Credential Blob are:

1. Credential Creation (Writing the Cred Blob)
    - A website (Relying Party, RP) asks the authenticator to create a new credential (authenticatorMakeCredential).
    - The RP provides a small data payload (up to 32 bytes) in the credBlob extension.
    - The authenticator securely stores this data alongside the newly created credential.
2. Credential Authentication (Reading the Cred Blob)
    - When a user authenticates (authenticatorGetAssertion), the RP can request the stored credBlob.
    - If the authenticator supports credBlob retrieval, it sends the stored blob back to the RP.
    - The RP can then use the data for credential management or additional verification.