uTrust FIDO2 Technical Manual

Table of Contents

Introduction to the uTrust FIDO2 Security Key Family

The uTrust FIDO2 Security Key Family offers strong authentication with support for multiple protocols, including FIDO2, which is the new standard that enables the replacement of password-based authentication. The uTrust FIDO2 strengthens security by replacing passwords with strong hardware-based authentication using public key cryptography.

- The full list of the services that work with uTrust FIDO2 is on Identiv's Works With uTrust FIDO2 page.
- Most of the rest of this guide targets systems integrators, IT teams, or developers who expect to integrate support for uTrust FIDO2 security keys into their environment.

All the security keys in the uTrust FIDO2 Security Key Family have the basic functionalities and capabilities described in this guide. However, it is the firmware version that determines which of the more specialized functionalities and capabilities are available to your key.

What's New?

The capabilities of the uTrust FIDO2 Security Key Family are dependent on the different combinations of firmware + connector type + protocol. This section covers connector types (form factors).

NFC

Expanding the options for quick tap-n-go authentication across desktops, laptops, and mobile devices, all of the applications - including FIDO2 - are available over NFC.

The uTrust FIDO2 NFC and uTrust FIDO2 NFC+ support the iPhone 7 and newer.

Background tag reading is supported in the iPhone XS and newer.

The uTrust FIDO2 NFC and uTrust FIDO2 NFC+ provide an NFC wireless interface In addition to USB. The uTrust FIDO2 NFC and uTrust FIDO2 NFC+ include the RFID standard specific to the ISO/IEC 14443-A and ISO/IEC 14443-4 NFC format; RFID implementations not included in the listed ISO standards are not supported.

For operations that require a touch, all touch requests within the first 20 seconds of the operation will succeed. After a period of inactivity, a security key placed on a desktop NFC reader may power

down to help prevent unintended access. To regain connectivity with an NFC reader, remove the key from the reader and reposition it on the reader. Some NFC readers may power-cycle and in doing so, prevent the key from powering down.

USB

All of the models in the uTrust FIDO2 Security Key Family provide a USB 2.0 interface, regardless of the form factor of the USB connector. The Security Key will present itself as a USB composite device in addition to each individual USB interface.

The USB PID string changes depending on which of the USB interfaces are enabled.

Firmware: Overview of Features & Capabilities

The uTrust FIDO2 security key firmware is separate from the uTrust FIDO2 security key itself in the sense that it is put onto each key in a process separate from the manufacture of the physical key. Nonetheless, it can be neither removed nor altered. Identiv periodically updates the uTrust FIDO2 security key firmware to take advantage of features and capabilities introduced into operating systems such as Windows, MacOS, and Ubuntu, etc., as well as to enable new uTrust FIDO2 security key features.

The firmware version on a uTrust FIDO2 security key therefore determines whether or not a feature or a capability is available to that device. The quickest and most convenient way to determine your device's firmware version is to use the uTrust Key Manager tool, a lightweight software package.

- Download the Key Manager tool: https://www.identiv.com/products/logical-access-control/utrust-fido2-security-keys/utrust-key-manager-software

The features, capabilities, and enhancements brought to the uTrust FIDO2 Security Key Family by the various firmware versions are **summarized** below, with the full details given in the technical description sections in this manual.

Secure Channel

Secure channel is used for establishing an authenticated and encrypted communication channel over CCID between a host and the secure element on the uTrust FIDO2 security key. The devices security domain can store three concurrent long-lived transport key sets.

SCP02, which is part of the GlobalPlatform standard, is a framework for mutual authentication and encrypted transport between hosts and secure elements in smart cards.

.

Benefits and Usage

- Encryption application keys can be stored on the CMS server as well as on the security key. If the key is lost or compromised, the encryption key can be recovered and loaded onto a replacement uTrust FIDO2 security key.
- Key diversification enables simplified and secured distribution of secure channel transport key sets as only the BMK must be shared with the CMS system to derive the uTrust FIDO2 security key transport key sets.
- Identiv can preprogram the secure channel transport key sets at the uTrust FIDO2 security key batches, if the key supply chain has access to the BMK of the CMS vendor.
- The CMS system can generate the secure channel transport key sets based on the uTrust FIDO2 security key serial numbers, the BMK, and additional metadata. The CMS can then use the initial secure channel transport key set for writing additional secure channel transport key sets to the security key.

Secure Channel CPLC Data

The Card Production Life Cycle (CPLC) data object is a random dataset that is stored on each uTrust FIDO2 security key to assure unique identification of the keys in CMS. Identiv has implemented the CPLC data object to provide unique identification of uTrust FIDO2 security keys for CMS vendors.

Physical Attributes

uTrust FIDO2 NFC and NFC+ Type A

- Dimensions: 48mm x 18mm x 4mm
- Weight: 3g
- Physical Interfaces: USB, NFC

- Operating Temperatures: 0 °C - 40 °C (32 °F - 104 °F)
- Storage Temperatures: -20 °C - 85 °C (-4 °F - 185 °F)

uTrust FIDO2 NFC and NFC+ Type C

- Dimensions: 43mm x 18mm x 4mm
- Weight: 3g
- Physical Interfaces: USB, NFC
- Operating Temperatures: 0 °C - 40 °C (32 °F - 104 °F)
- Storage Temperatures: -20 °C - 85 °C (-4 °F - 185 °F)

Understanding the USB Interfaces

USB interfaces are the different channels that software can use to communicate with the uTrust FIDO2 key when it is connected via USB. Each interface enables a specific set of applications on the security key.

OTP

The OTP interface presents itself to the operating system as a USB keyboard. The OTP application is accessible over this interface. Output is sent as a series of keystrokes from a virtual keyboard. This allows OTP to be used in any environment that can accept standard keyboard input.

The OTP interface is supported natively across all desktop OS environments (macOS, Windows, Linux) as well as on mobile OS platforms (iOS, Android). Output is sent as a series of keystrokes from a virtual keyboard, allowing the OTP application to work with any environment that supports USB keyboard input.

FIDO

The FIDO interface provides access to the FIDO2 and U2F applications.

The FIDO interface presents itself as a generic human interface device (HID). The FIDO interface is supported on all desktop platforms running WebAuthn-compatible browsers or applications, as well as on Android and iOS (starting in iOS 13).

CCID

The CCID interface provides communication for the PIV / Smart Card, and OATH (HOTP and TOTP).

The uTrust FIDO2 NFC/NFC+ presents itself to the operating system as a USB smart card reader. The CCID interface is supported on Windows and MacOS, and on Linux with the PC/SC package. CCID is also supported on Android.

Protocols and Applications

The uTrust FIDO2 Security Key Family provides applications for FIDO2, OATH, Smart Card, U2F. The applications are all separate from each other, with separate storage for keys and credentials.

Note that the OATH categories overlap; technically, there are two true OTPs:

- OATH-HOTP (standard RFC4226)
- OATH-TOTP (standard RFC6238)

FIDO2

The FIDO2 standard offers the same high level of security as FIDO U2F, since it is based on public key cryptography. In addition to providing phishing-resistant two-factor authentication, the FIDO2 application on the key allows for the storage of resident credentials, also called discoverable credentials. As these credentials can accommodate the username and other data, this enables truly passwordless authentication on sites and applications that support the WebAuthn protocol.

FIDO2 support is available to the iPad Pro via the USB-C connector of the uTrust FIDO2 Security Key. FIDO2/WebAuthn can be achieved over USB-C using any of the following options:

- `ASWebAuthenticationSession`
- `SFSafariViewController`
- Redirect to Safari browser

Locking FIDO2 Credentials

The resident credentials can be left unlocked and used for strong single-factor authentication, or they can be protected by a PIN for two-factor authentication.

- The FIDO2 PIN must be between 4 and 63 characters in length.
- Once a FIDO2 PIN is set, it can be changed but it cannot be removed without resetting the FIDO2 application.
- If the PIN is entered incorrectly 8 times in a row, the FIDO2 application will be locked. In order to restore this functionality, the FIDO2 application must be reset.

NOTE:
Resetting the FIDO2 application will also reset the U2F key, so the security key must be re-registered not only with all the FIDO2 sites, but also with all U2F sites.

Default Values

PIN: None set.

AAGUID Values

NFC and NFC+models: 73402251-f2a8-4f03-873e-3cb6db604b03

FIDO U2F

FIDO U2F is an open standard that provides strong, phishing-resistant two-factor authentication for web services using public key cryptography. U2F does not require any special drivers or configuration to use, just a compatible web browser. The U2F application on the key can be associated with an unlimited number of U2F sites.

OATH

The OATH application can store one OATH credential, either OATH-TOTP (time-based One-Time Password) or OATH-HOTP (counter-based One-Time Password).

HOTP and TOTP

Both **OATH-TOTP** and **OATH-HOTP** credentials are described in detail in the OATH Overview.

Smart Card (PIV Compatible)

The uTrust FIDO2 Security Key Family provides a PIV-compatible smart card application. PIV, or FIPS 201, is a US government standard. It enables RSA or ECC sign/encrypt operations using a private key stored on a smart card through common interfaces like PKCS#11.

On Windows, the smart card functionality can be extended with the uTrust Smart Card Minidriver (coming soon).

The uTrust FIDO2 Security Key Family supports extended APDUs, extended `Answer To Reset (ATR)`, and `Answer To Select (ATS)`.

Default Values

- PIN: 123456
- PUK: 12345678
- Management Key (3DES): `010203040506070801020304050607080102030405060708`

Supported Algorithms

The uTrust FIDO2 Security Key Family supports the following algorithms on the PIV smart card application.

- RSA 1024
- RSA 2048
- RSA 3072
- ECC P-256
- ECC P-384

Policies

PIN Policy

To specify how often the PIN needs to be entered for access to the credential in a given slot, set a PIN policy for that slot. This policy must be set upon key generation or import; it cannot be changed later.

Slot Information

The keys and certificates for the smart card application are stored in slots, which are described below. The PIN policies described below are the defaults, before they are overridden with a custom PIN policy. **These slots are separate from the programmable slots in the OTP application.**

Slot 9a: PIV Authentication

This certificate and its associated private key is used to authenticate the card and the cardholder. This slot is used for system login, etc. To perform any private key operations, the end user PIN is required. Once the correct PIN has been provided, multiple private key operations may be performed without additional cardholder consent.

Slot 9c: Digital Signature

This certificate and its associated private key is used for digital signatures for the purpose of document, email, file, and executable signing. To perform any private key operations, the end user PIN is required. The PIN must be submitted immediately before each sign operation to ensure cardholder participation for every digital signature generated.

Slot 9d: Key Management

This certificate and its associated private key is used for encryption to assure confidentiality. This slot is used for encrypting emails or files. The end user PIN is required to perform any private key operations. Once the correct PIN has been provided, multiple private key operations may be performed without additional cardholder consent.

Slot 9e: Card Authentication

This certificate and its associated private key is used to support additional physical access applications, such as providing physical access to buildings via PIV-enabled door locks. The end user PIN is NOT required to perform private key operations for this slot.

Tools and Troubleshooting

uTrust Key Manager

The uTrust Key Manager is a tool for configuring all aspects of uTrust FIDO2 security keys and for determining the model of key and the firmware it runs. It has both a graphical interface and a command line interface.

Graphical User Interface (GUI)

The graphical user interface of the uTrust FIDO2 Key Manager provides an easy-to-use method of performing basic configuration tasks of the uTrust FIDO2 Security Key Family, including:

- Displaying information about the key(s) connected to the computer.
- Setting or changing the FIDO2 PIN, as well as resetting the FIDO application.
- Managing the credentials in the OTP application.

Troubleshooting

If you run into any issues with a key from the uTrust FIDO2 Security Key Family, refer to the Knowledge Base and search for your issue. If your issue is not listed in the Knowledge Base, or if you have any technical questions, you can get in touch with Identiv Support by clicking here.

FIDO2 AAGUIDs

The FIDO2 specification states that an Authenticator Attestation GUID (AAGUID) must be provided during attestation. An AAGUID is a 128-bit identifier indicating the type of the authenticator.

New AAGUIDs will be issued for new Identiv products which support FIDO2, or when existing uTrust FIDO2 products have FIDO2 features added or removed.

For the AAGUIDs, see AAGUID Values section above.

Global Platform: CPLC Data

Description

Although this format is officially deprecated and not part of the GlobalPlatform specification, some organizations need support for the information stored in the so-called CPLC (Card Production Life Cycle).

This consists of a static set of bytes can can be retrieved with a GET DATA command (INS 0xca) and TAG 0x9f7f after selecting the SD application.

The response is 42 bytes that can be parsed into different fields with different meanings. However, Identiv elected not to attribute any specific meaning to 40 of those bytes. Only the first two bytes are meaningful.

Example Command

To retrieve the value (scroll horizontally if necessary):

```
opensc-tool -c default -s '00a4040008a000000151000000' -s '00ca9f7f'
```

Relevant Output

```
40 90 73 F9 53 94 C0 01 23 D8 E9 F0 68 3A 48 9A    @.s.S...#...h:H.
76 30 4C D8 F6 CC 41 66 61 0F C4 F5 8C DE D6 93    v0L...Afa.......
77 32 09 82 1B EA 0C 78 3D 8B                      w2.....x=.
```

Of those 42 bytes, only the first two (40 90) are meant to signify an Infineon SLE 78 chipset, the rest are random bytes generated when the SD application is (re)initialized.

Acronyms

3DES	Triple Data Encryption Algorithm
AES	Advanced Encryption Standard
CCC	Card Capability Container
CCID	Chip card interface device, a USB protocol for a smartcard.
CHUID	Card Holder Unique ID
CMS	Credential Management System
CN	Common name
CSR	Certificate Signing Request
ECC	Elliptic curve cryptography

FIDO	Fast Identity Online
FIPS	Federal Information Processing Standards (US government) covering codes and encryption standards.
HMAC	Hash-based message authentication code
HOTP	HMAC-based One-Time Password algorithm
KDF	Key Derivation Function
OATH	The Initiative for Open Authentication is an organization that specifies two open authentication standards, TOTP and HOTP.
OTP	One-Time Password
PBKDF2	Password-Based Key Derivation Function 2
PKCS #11	This is number eleven of the Public Key Cryptography Standards; it is also the API for creating and manipulating cryptographic tokens.
PUK	PIN Unlock Key
stdin	standard input - usually keyboard or CLI instructions
stdout	standard output - usually print to screen
TOTP	Time-based One-Time Password algorithm
X.509	The standard defining the format of a public key certificate