Idem Key
Technical Specification

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, contact support@GoTrustID.com.

Date May-5-2025

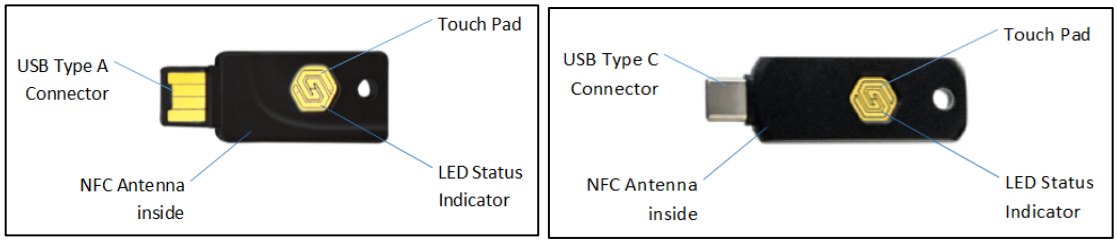
Contents

1 Overview of GoTrust Idem Key

GoTrust Idem Key, hereinafter referred to as Idem Key, is a cutting-edge product designed to secure user identity and enable phishing resistant two-factor authentication (2FA) across mobile devices and workplace environments. It incorporates a wide range of features and supports multiple security standards to meet enterprise and individual security needs.

Key features include:

- **FIDO2 and FIDO U2F Authentication**: As part of GoTrust's FIDO series, Idem Key enables seamless authentication to all FIDO U2F and FIDO2-compatible services such as Microsoft Entra ID, M365, Google, AWS, Facebook, Amazon, X (Twitter), Dropbox, and many others, through USB or NFC-enabled devices.
- **Smart Card (PIV) Functionality**: Idem Key supports Personal Identity Verification (PIV) standards, enabling certificate-based authentication, digital signatures, and secure email encryption. It is compatible with major operating systems and enterprise PKI environments, providing strong authentication for smart card logon and VPN access.
- **OATH HOTP Support**: Idem Key supports OATH HOTP (HMAC-Based One-Time Password) functionality, allowing users to perform secure event-based OTP authentication with services and systems that support hardware tokens.
- **User Presence Verification**: Idem Key requires a user touch operation to authorize authentication requests, ensuring an additional layer of security.
- **Universal Form Factors**: Designed in standard USB Type-A and Type-C form factors, Idem Key is compatible with a wide range of laptops, desktops, and mobile devices.
- **FIPS validated algorithms:** All cryptographic operations are performed using FIPS-validated algorithms within a FIPS 140-2 certified cryptographic module.



Outlook of Idem Key

2 Specification of Idem Key-A

- Application: FIDO2, FIDO U2F, PIV, and OATH HTOP
- Dimensions: 48.2mm x 18.3mm x 4.1mm
- Weight: 4g / 9.2g (with package)
- Physical Interfaces: USB Type A, NFC
- Operating Temperatures: 0°C ~ 40°C (32°F ~ 104°F)
- Storage Temperatures: -20°C ~ 85°C (-4°F ~ 185°F)
- Compliance
    - FCC
    - CE
    - RoHS
    - WEEE
    - IP68
- Certification:
    - FIDO2 Security Level 2 and FIDO U2F
    - Secure element is FIPS 140-2 Level 3 certified

3. Specification of Idem Key-C

- Application: FIDO2, FIDO U2F, PIV, and OATH HTOP
- Dimensions: 50.4mm x 16.4mm x 5mm
- Weight: 5g / 10.5g (with package)
- Physical Interfaces: USB Type C, NFC
- Operating Temperatures: 0°C ~ 40°C (32°F ~ 104°F)
- Storage Temperatures: -20°C ~ 85°C (-4°F ~ 185°F)
- Compliance
    - FCC
    - CE
    - RoHS
    - WEEE
    - IP68
- Certification:
    - FIDO2 Security Level 2 and FIDO U2F
    - Secure element is FIPS 140-2 Level 3 certified

4 FIDO Features

FIDO2 Certification

Both Idem Key-A and Idem Key-C are certified by FIDO U2F and FIDO2 Security Level 2 standard which conforms with CTAP 2.0 specification. The CTAP 2.1 version will be ready in July 2025.

FIDO2 Credentials

Idem Key supports FIDO2 PIN functionalities with following features.

- FIDO2 PIN does not exist on the new Idem Key. User needs to set PIN himself.
- FIDO2 PIN must be between 4 and 63 characters in length.
- FIDO2 PIN will be locked after subsequence 8 times incorrect PIN entered.
- Once the PIN is locked, user must reset Idem Key to restore the functionality. However, all the credentials (include U2F credentials) will be erased after reset.

Capacity to Store FIDO2 Passkeys

Idem Key can store up to **30 passkeys** in it.

FIDO2 AAGUID

In FIDO2 specification, it defines an Authenticator Attestation GUID (AAGUID) to be used during the authenticator attestation process. AAGUID consists by a 128 bits identifier.

Product	AAGUID
Idem Key - A	3b1adb99-0dfe-46fd-90b8-7f7614a4de2a
Idem Key - C	e6fbe60b-b3b2-4a07-8e81-5b47e5f15e30

5 PIV (Smart Card Functionality) Support in Idem Key

Idem Key implements core features of the Personal Identity Verification (PIV) standard (FIPS 201) to provide smart card-based authentication, digital signatures, and encryption capabilities.

Its PIV functionality is offering strong compatibility with enterprise PKI and smart card environments.

The following list outlines the PIV features supported by Idem Key:

Supported Features

- Smart Card (PIV) authentication (PKI-based login to Windows, macOS, and Linux systems)
- Digital signature generation (using private keys stored securely on the device)
- Email and document encryption/decryption (S/MIME support)
- Certificate-based VPN authentication
- SSH authentication with PIV keys
- PIN-protected private key usage (per PIV specifications)
- Management Key protection for administrative operations

Cryptographic Capabilities (FIPS-Validated Algorithms)

- RSA: 2048-bit key support
- ECC: P-256 and P-384
- AES-128, AES-192, AES-256
- 3DES
- SHA-1 and SHA-256

Key Slots

- PIV Authentication (Slot 9a)

- Digital Signature (Slot 9c)
- Key Management (Slot 9d)
- Card Authentication (Slot 9e)
- Additional Retired Key Management Slots (82–95)

Supported Middleware and Software

- Idem Key Minidriver (Windows 10/11)
- Microsoft Windows Smart Card Services
- macOS Smart Card Services
- Linux OpenSC (PKCS#11 interface), supporting smart card login (PAM), browser-based authentication (Firefox), digital signature and encryption (GnuPG), and VPN authentication (e.g., OpenVPN)
- Middleware solutions compatible with PKCS#11 or PIV standards
- Certificate enrollment through Microsoft Certificate Services and third-party PKI systems (Windows platforms require Idem Key Minidriver)

6 Supported Platform

Operating System	Interface	Support Details
Windows 10 / 11	USB / NFC	Supports FIDO2, U2F, and PIV (via Idem Key Minidriver); compatible with Windows Hello and external NFC readers
macOS 10.15+	USB	Supports FIDO2, U2F, and native PIV Smart Card Login via Safari, Chrome, Firefox, Opera, and Edge
Linux	USB	Supports FIDO2, U2F, and PIV via OpenSC and PKCS#11-compatible applications
Android 8.0+	USB-C / NFC	Supports FIDO2 and U2F via Chrome and supported apps; USB-C requires OTG support
iOS 13.3+	NFC	Supports FIDO2/WebAuthn via Safari, Chrome, Firefox, Opera, and Edge
ChromeOS 75+	USB	Supports FIDO2 and U2F for Google account login via Chrome OS login screen and browser.

Note:

- Safari, Chrome, Firefox, Opera, and Edge on iOS and macOS support FIDO2/WebAuthn; implementation details may vary slightly between browsers.
- USB interface is supported on all major desktop platforms.
- Mobile platforms support either USB-C (with OTG) or NFC, depending on hardware capability.
- PIV support on Windows requires installation of the Idem Key Minidriver.

7 Supported Applications

The following applications are compatible with Idem Key, categorized by supported protocol. Please note that the listed applications represent commonly used platforms and systems for which Idem Key has been verified to interoperate. This list is not exhaustive, as FIDO-compatible services are continually expanding.

Protocol	Supported Applications	
FIDO2 / U2F	Google Workspace	Google
	Microsoft 365 / Azure AD	Microsoft
	Dropbox	Dropbox Business
	GitHub	GitHub
	Facebook	
	X (Twitter)	
	Cloudflare	CLOUDFLARE
	Okta	okta
	Auth0	Auth0
	Salesforce	salesforce
	Shopify	shopify
	Namecheap	namecheap
	GoDaddy	Go Daddy
	Proton	Proton
	Tuta	tuta
	Fastmail	Fastmail
	1Password	1Password
	Bitwarden	bitwarden

Protocol	Supported Applications	
	Login.gov	LOGIN.GOV
	ID.me	ID.me
	Coinbase	coinbase
	Kraken	kraken
	Binance	BINANCE
	Bitfinex	BITFINEX
	Bank of America	BANK OF AMERICA
PIV (Smart Card)	Windows Smart Card Logon (requires Idem Key Minidriver), macOS Smart Card Login (native), Linux (PAM modules, OpenSC), Active Directory Certificate Services (AD CS), Citrix Virtual Apps and Desktops, VMware Horizon	Windows platforms require Idem Key Minidriver installation.
OATH HOTP	Duo Security and CyberArk Identity	Requires pre-provisioned secrets; dependent on platform support.