EVIDEN

CardOS Security Token

FIDO2 and PKI with CardOS USB Token

Overview

With the CardOS Security Token, Eviden offers a USB token solution for PKI and FIDO2 applications, featuring a crypto chip for security functions, cryptographic operations, and secure creation and storage of cryptographic keys and certificates.

CardOS showcases Eviden's extensive expertise as both a European-leading systems integrator and a leader in smart card development.

Based on CardOS USB V5.6, the CardOS Security Token includes a contactless communication interface in addition to the USB interface. This solution seamlessly fits into IT environments with mobiles, tablets, and notebooks that lack an internal smart card reader.

Highlights

CardOS Security Token – PKI

Based on Public Key Infrastructure (PKI), cryptographic keys and certificates are essential for securing today's online activities. PKI is used for secure email, digital signatures, authentication to services, and logging into workstations.

CardOS Security Token supports this by securely creating, storing, and using keys and certificates to perform all necessary security operations.

Together with separately available smart card middleware (CardOS API, SCinterface), CardOS Security Token offers an ideal, easy-to-use solution for securing standard applications. The smart card middleware, with its standard interfaces, enables seamless integration and use of the stored keys and certificates in standard applications on Windows, Linux, and macOS.

CardOS Security Token – FIDO2

Passwords are often deemed inadequate and are considered the weak link in authentication by security experts, as they can be compromised more easily than other methods. Creating strong and unique passwords for each account quickly becomes a challenge for users. The 2021 Verizon Data Breach Investigation Report[1] stated that 61% of breaches involved credentials, with 25% using stolen credentials.

Eviden offers FIDO2 to address these challenges, enabling users to log in to their applications and services with much higher security. This allows organizations to implement two-factor authentication with FIDO2, combining something you have (the token) with something you know (the secret token PIN) for secure authentication.

The CardOS Security Token provides the advantage of using one authenticator for multiple logins to different applications, requiring only one PIN to enable access to the authenticator. The CardOS Security Token is designed for customers in the public or enterprise market. Secure, convenient password-less authentication is a growing trend, and many services already offer the option to use FIDO2 authentication.

Hardware and OS platform

CardOS USB V5.6, the smart card OS platform used in the CardOS Security Token, is based on Infineon's innovative digital security technology 'Integrity Guard' and is implemented on the SLE78 security controller platform. The chip used is the SLE78CLUFX5000PHM, with which around 160 kB of user memory is available.

CardOS USB V5.6 is a multifunctional native smart card operating system, expandable by customized packages to enhance or modify its functionality. It offers state-of-the-art cryptographic algorithms, including AES, SHA-2, and elliptic curves.

[1] www.verizon.com/business/resources/reports/dbir/

What is FIDO2[2]?

FIDO2 (Fast IDentity Online) offers a secure, convenient, and straightforward authentication method. FIDO2 specifications aim to eliminate the risks of password theft and phishing attacks.

The user registers to a web application or service

His/Her registration generates a public key and a private key

When requesting access to the web service, a challenge is generated

The challenge is signed with key data for the web service and returned

The user can successfully login

CardOS Security Token as FIDO2 Authenticator

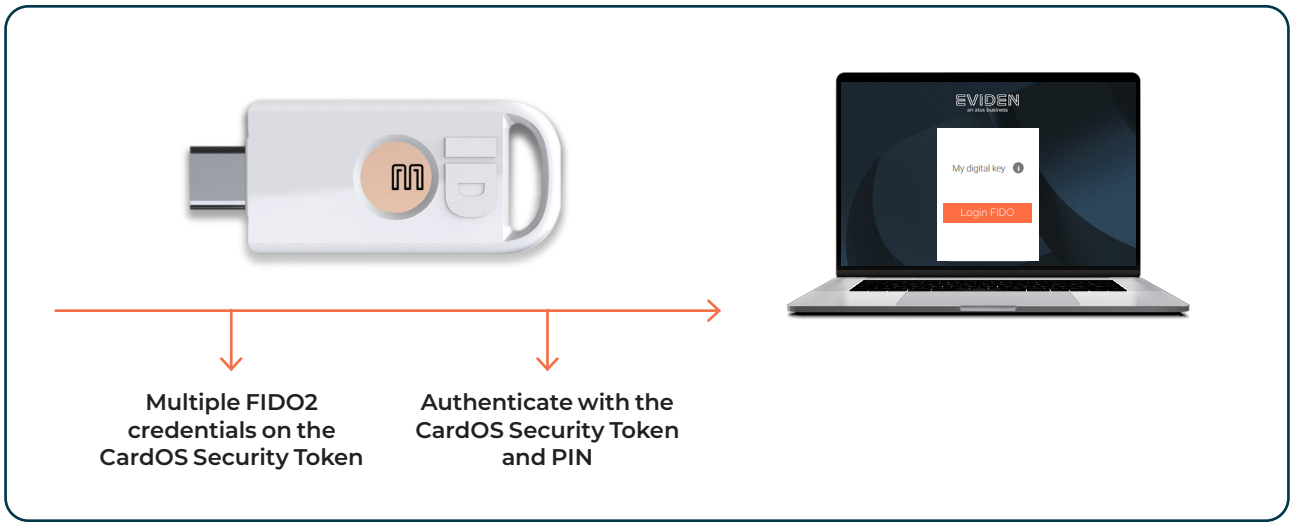
With the CardOS Security Token, Eviden offers a FIDO2 Authenticator based on the CardOS USB V5.6 operating system, compliant with FIDO2 specifications and certified by the FIDO™ Alliance.

FIDO2 authentication relies on public key cryptography. Leveraging the robust security mechanisms of CardOS, the keys used for authentication are created within the CardOS chip and never leave it.

Supporting the FIDO2/CTAP[3] protocol, the CardOS Security Token enables passwordless authentication for services accepting or requiring FIDO authentication.

The CardOS Security Token provides a secure and convenient solution for passwordless authentication. End users need only authenticate with their CardOS Security Token and a PIN, if required by the server, eliminating the need to remember passwords and login names. This also helps lower helpdesk costs related to password resets.

[2] The FIDO, FIDO ALLIANCE, FIDO AUTHENTICATION, FIDO CERTIFIED and FIDO2 trademarks and logos are trademarks of FIDO Alliance.
[3] Client To Authenticator Protocol (CTAP) is a specification enabling communication between a client and an external authenticator.



CardOS Security Token for a variety of applications

The CardOS Security Token is perfect for IT environments and devices without an integrated smart card reader, eliminating the need for an additional card reader compared to smart-card-based solutions. It supports various authentication options, including PKI functionality, OTP, and FIDO, in any combination:

- **CardOS Security Token as FIDO 2 Authenticator**
- **CardOS Security Token as FIDO2 Authenticator with integrated PKI functionality (PKCS#15, CardOS API / SC interface)**
- **CardOS Security Token as FIDO2 Authenticator with PKI and OTP (for use with CardOS SmartOTP)**
- **CardOS Security Token with PKI and optional OTP**

CardOS Security Token - Connectivity

The CardOS Security Token offers two connectivity options: USB and the built-in contactless interface. This enables the token to connect with mobile devices via their NFC interface.

Additionally, the contactless interface of the CardOS Security Token supports physical access solutions through MIFARE Classic Emulation of a 4k MIFARE chip.

Communication protocols

USB protocols:

- CCID
  - for the usage with commonly installed reader drivers on Windows, Linux and macOS
  - for standard enterprise usage with smart card middleware, CardOS API / SC interface with standard applications that use the interfaces Minidriver, PKCS#11 and CTK
- HID
  - to support the FIDO2.0/2.1 authenticator specification

Transmission protocol according to ISO/IEC:

- T=CL (ISO/IEC 14443-4 protocol Type A)
- Support of extended length APDUs according to ISO/IEC 7816-4
- Contactless card communication with up to 848 kbaud
- NFC Tag Type 4

Tools and support

To help with the integration of CardOS Eviden provides customers with:

- Manuals and script files
- Script tool for executing card commands and loading packages
- Professional Service:
  - Professional support for integration projects
  - Customized Packages and File Structures
- CardOS API or SCinterface, the standard cryptographic interface middleware for CardOS token with Microsoft Base CSP and PKCS#11 support
- CardOS SmartOTP, the software app for OTP calculation
- Delivery of complete turn-key solutions for registration, usage and revocation of CardOS Security Tokens

Standards and technical highlights

Communication Interfaces

- USB 2.0:
  - USB Type A Connector
  - USB Type C Connector
- NFC:
  - T=CL (ISO14443/IEC 14443-4 Type A)

Certifications

- FIDO2 Level 1

Supported operating systems*

- Windows 10, 11
- Linux
- macOS
- Android
- iOS

* Not all applications might be supported

Dimensions

- USB Type A: 52 x 20 x 5 mm
- USB Type C: 48 x 20 x 5 mm

Temperature range

- Operating temperature range: 0°C to +40°C
- Storage temperature range: -20°C to +85°C

Connect with us

/in/eviden
@EvidenLive
@evidenlive
/EvidenLive

eviden.com