

# Top 5 Reasons choosing SafeNet eToken Fusion Series

## Phishing-Resistant FIDO2 & PKI Authentication from Any Device



FIDO authentication has gained traction as a modern form of MFA due to its benefits in easing the end-user login experience and overcoming password vulnerabilities. However, many organizations have invested heavily in Public Key Infrastructure (PKI) for use cases such as digital signing or email encryption, which FIDO cannot replace. Here are the top five reasons why you should consider SafeNet eToken Fusion security keys.

The SafeNet eToken Fusion series is a set of USB tokens combining FIDO2 with PKI in a single authenticator



## 01 Prevent phishing attacks

Relying on asymmetric public key cryptography and possession-based authentication, FIDO2 and PKI Certificate-Based-authentication (CBA) are phishing-resistant authentication technologies that provide protection against Phishing and Man-In-The-Middle attacks (MiTM) attacks.

## 02 Get the best from PKI and FIDO worlds

With the SafeNet eToken Fusion series, you can deploy FIDO authentication to securely and easily access modern applications or Windows desktops, while retaining PKI use cases such as CBA for legacy computing resources, digital signatures and files encryption.



## 03 Deploy on any device – mobile or laptops

SafeNet eToken Fusion USB-C and USB-A are compatible with any laptop or mobile device. Your end users can securely access to sensitive resources from anywhere.



## 04 Make life easier for your users and your IT

PKI and FIDO2 are passwordless authentication methods, so users don't need to remember passwords, reducing help for many operations. FIDO2 is an open standard that makes SafeNet eToken Fusion compatible with any IAM platform that supports FIDO2.



## 05 Comply with your markets' regulations

The SafeNet eToken Fusion series is FIDO2 certified and comply with Common Criteria, eIDAS and French ANSSI. This lets you comply with the most stringent regulatory requirements.

