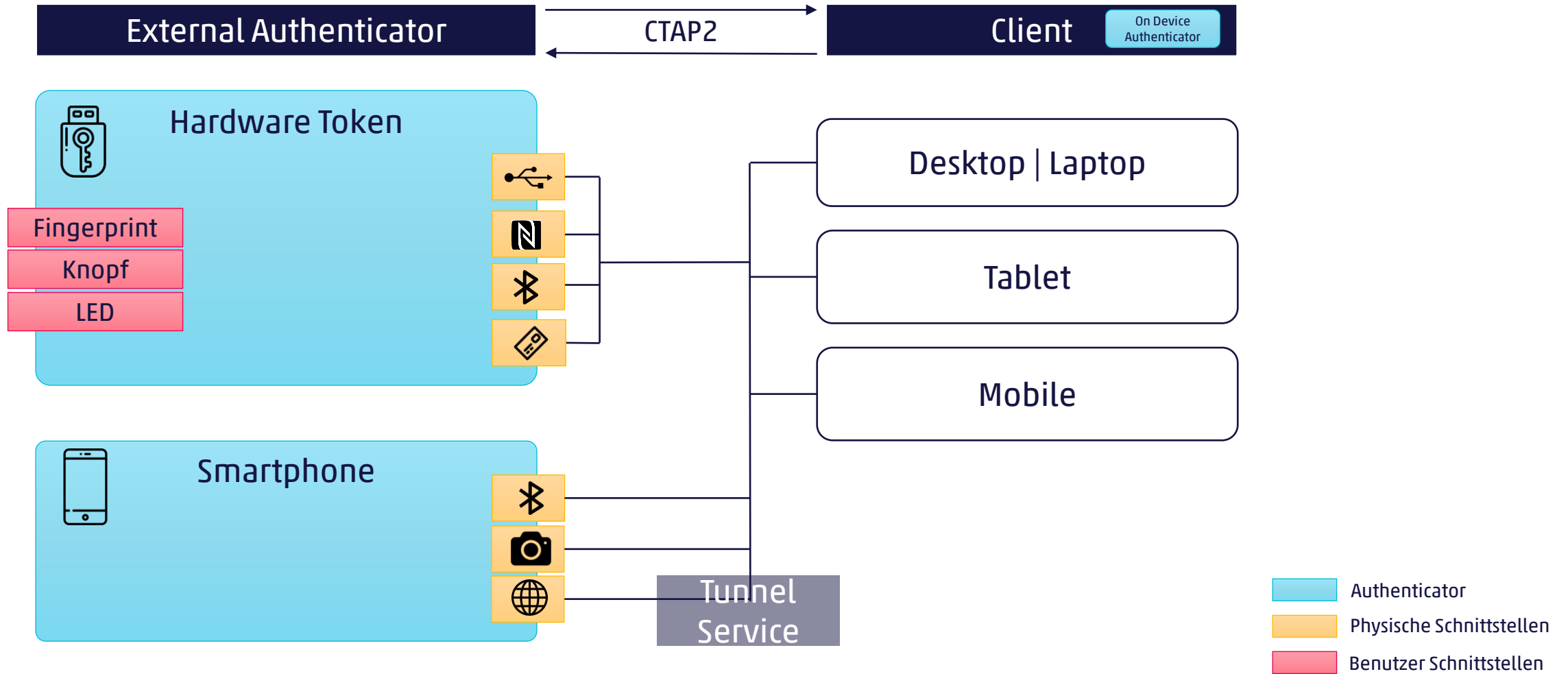


Authenticators

Pasqualino Casciano

cnlab Herbsttagung 2025 – FIDO2: einfach und sicher
Gleisarena, Zürich, 3. September 2025

Authenticator Arten



Beispiele (Hardware-Token)

	Produktname	Hersteller	Preis
	YubiKey 5C Nano	Yubico	78 CHF
	YubiKey C Bio-FIDO	Yubico	112 CHF
	VeriMark Guard	Kensington	56 CHF
	iShield Key Pro	Swissbit	84 CHF
	StarSign Key Fob	G+D	56 CHF
	3A Mini	Nitrokey	71 CHF



Hauptfunktionen

Management

Funktionen

- Token auf die Werkeinstellungen zurücksetzen
- PIN setzen und PIN ändern
- Fingerabdrücke registrieren
- Passkeys löschen

Mit herstellerspezifischer Software oder mit Betriebssystem-Mitteln

Registrierung

- Schlüsselpaar erzeugen
 - Discoverable (bis zu 100 Schlüssel können lokal gespeichert werden)
 - Non-discoverable (unlimitiert)

Authentisierung

- Challenge beantworten

Allgemein

- User-Verifikation (PIN, Biometrie)
- User-Presence prüfen

Management-Software (Hardware-Token)

Produktname	Hersteller	Management-Software
YubiKey 5C Nano	Yubico	Yubikey Authenticator und Kommandozeilen-Tool
YubiKey C Bio-FIDO Edition	Yubico	Yubikey Authenticator und Kommandozeilen-Tool
VeriMark Guard	Kensington	nur für macOS
iShield Key Pro	Swissbit	iShield Key Manager
StarSign Key Fob	G+D	Mobile App (iOS, Android)
3A Mini	Nitrokey	Nitrokey App und Kommandozeilen-Tool

Die Management-Software wird auf einem PC oder Mac installiert und muss als Administrator ausgeführt werden. In der Regel verfügt die Management-Software über eine Benutzeroberfläche (GUI), es gibt aber auch Kommandozeilen-Tools.



PIN

- Mindestens 4 Zeichen (alphanummerisch), vom Standard verlangt
- PIN-Eingabe kann vom Authenticator und/oder von der RP verlangt werden.
- Die PIN-Eingabe kann im Authenticator ausgeschaltet werden.
- Der Standard verlangt nicht, dass eine Benutzerverifikation stattfinden muss.
- Einzelne Hersteller haben eine höhere untere Grenze für die PIN-Länge (z.B. Yubikey verlangt mindestens 6 Zeichen bei ausgewählten Modellen)
- Maximale PIN-Länge hängt vom Hersteller ab (bei Yubikey ist diese auf 64 Zeichen begrenzt)
- Beschränkung der Anzahl der Fehlversuche. Typischerweise wird der Hardware-Token nach acht Fehlversuchen gesperrt (z.B. Yubikey, Nitrokey, Swissbit). Danach muss das Hardware-Token zurückgesetzt werden
- Komplexitätsregeln werden teilweise unterstützt (z.B. von Yubikey ab Firmware Version 5.7)



Fingerabdrücke

- Yubikey Bio: Es können 5 Fingerabdrücke registriert werden, nachdem eine PIN gesetzt worden ist.
- VeriMark Guard: Es können 10 Fingerabdrücke registriert werden (gemäss Herstellerangaben).
- StarSign Key Fob: Es können 20 Fingerabdrücke registriert werden (gemäss Herstellerangaben). Für die Erfassung eines neuen Fingerabdruckes ist eine PIN-Eingabe nötig.

FIDO-Alliance-Zertifizierung für Authenticators (1/2)

	HW & SW Requirements	Defend against	Implementation examples
L1	Any device HW or SW	L1 prevents against phishing and the majority of scalable attacks with software and security best practices.	L1 is the by-default security level required for any functional certification.
L2	Device must support allowed ROE (e.g. TEE, Secure Element...), as listed here .	L2 authenticators with a hardware protected border (AROE), protecting against remote software attacks.	Within the list of Allowed ROE: • Security Key (BLE/NFC/USB) • TEE based on ARM Trustzone • TEE Based on Intel VT HW...
L3	Device supported by an AROE with security resistance against physical attacks.	L3 authenticators with a hardware protected border (AROE), protecting against remote software attacks and local hardware attacks.	GlobalPlatform certified TEE (L3 GlobalPlatform Companion Program) CC certified Secure Element (L3 CC Companion Program)

<https://fidoalliance.org/certification/>

Zertifizierung für Authenticators (2/2)

FIDO Authenticator Certification Examples		
L3+	 USB U2F Token built on a CC-certified Secure Element Certification: L3+	
L3	 USB U2F Token built on a basic simple CPU, OS, is certified. Good physical anti-tampering enclosure  UAF implemented as a TA running on a certified TEE with POP memory	
L2	 UAF implemented as a TA in an uncertified TEE	
L1+	 UAF in downloadable app using white box crypto and other techniques Certification: L1+	
L1	 Downloaded app making use of Touch ID on iOS Certification: L1  FIDO2 making use of the Android keystore. Keystore is not certified Certification: L1  FIDO2 built into a downloadable web browser app Certification: L1	

0

~70

0

~270



Metadata-Service (MDS)

- <https://fidoalliance.org/specs/mds/fido-metadata-service-v3.1-ps-20250521.html>
- Signierte Datei (JWT), die von der FIDO-Alliance zur Verfügung gestellt wird.
- Wird monatlich aktualisiert
- Identifikation des FIDO2-Authenticators über die AAGUID
- Enthält Zertifikate für die Validierung der Attestation (Signaturen)
- Informationen zu den Authenticators wie z.B.
 - FIDO-Zertifizierungslevel: L1, L2 oder L3
 - Angabe zu den unterstützten Authentisierungsmethoden (PIN, Biometrie)
 - Angaben zur PIN (Länge, Anzahl Fehlversuche)
 - Art des Schlüsselschutzes (Hardware, Software)
 - Weitere Angaben zum Authenticator: Anschlussmöglichkeiten (z.B. USB oder NFC), Unterstützung für „discoverable keys“

AAGUIS (Authenticator Attestation Globally Unique ID)

	Hersteller	AAUID
YubiKey 5C Nano	Yubico	ff4dac45-edc8-4ec2-aced-cf66103f4335
YubiKey C Bio-FIDO Edition	Yubico	dd86a2da-86a0-4cbe-b462-4bd31f57bc6f
VeriMark Guard	Kensington	d94a29d9-52dd-4247-9c2d-8b818b610389
iShield Key Pro	Swissbit	5d629218-d3a5-11ed-afa1-0242ac120002
StarSign Key Fob	G+D	f8d5c4e9-e539-4c06-8662-ec2a4155a555
iPhone X	Apple	fbfc3007-154e-4ecc-8c0b-6e020557d7bd
3A Mini	Nitrokey	2cd2f727-f6ca-44da-8f48-5c2e5da000a2

Schnittstellen, Zertifizierung und Besonderheiten

Produktname	Hersteller	Schnittstellen	Zertifizierung	Besonderheiten
YubiKey 5C Nano	Yubico	USB-C	L2	Kleiner Formfaktor
YubiKey C Bio-FIDO	Yubico	USB-C	L2	Fingerabdruck
VeriMark Guard	Kensington	USB-C	L1	Fingerabdruck
iShield Key Pro	Swissbit	USB-C, NFC	L1	
StarSign Key Fob	G+D	USB-C, Bluetooth	-	Fingerabdruck Firmware-Update
iPhone X	Apple	QR-Code, Bluetooth, Internet	-	
3A Mini	Nitrokey	USB-A	L1	Open Source, Firmware-Update



Vielen Dank für Ihre Aufmerksamkeit_

Pasqualino Casciano
pasqualino.casciano@cnlab.ch

info@cnlab-security.ch
+41 55 214 33 40

cnlab security AG
Obere Bahnhofstrasse 32b
CH-8640 Rapperswil-Jona
Switzerland