Vier FIDO2-Token für den USB-Port

Vier FIDO2-Token für den USB-Port

Für eine Zwei-Faktor-Authentifizierung, die nicht an ein bestimmtes Endgerät wie ein Mobiltelefon oder einen PC gebunden sein soll, bieten sich USB- oder NFC-Token als Roaming-Devices an. Wir haben uns vier davon näher angesehen.

Von Jürgen Seeger

Auf dem Markt gibt es eine niedrig dreistellige Zahl von als Security Keys oder FIDO-Sticks bezeichneten Token. Für unsere Betrachtung haben wir OTP-Generatoren, bei denen man eine erzeugte PIN von einem Display abtippen muss, von vornherein aussortiert. Denn eine NFC- oder USB-Anbindung macht das Handling deutlich einfacher – dranhalten oder reinstecken reicht.

In die engere Auswahl kamen vier solcher Keys – und zwar die aus der Kompatibilitätsliste von Microsoft (siehe ix.de/zm8b) –, deren Hersteller FIPS-zertifizierte Produkte im Portfolio haben. In den Federal Information Processing Standards (FIPS) sind die Anforderungen von US-Behörden an IT-Equipment veröffentlicht, FIPS 140-2 und der Nachfolger 140-3 behandeln die Sicherheit kryptografischer Module, getestet in einem fünfstufigen Prozess. US-Behörden betrachten Sicherheitsmodule ohne ein solches Zertifikat juristisch als unsicher, eine mit nicht FIPS-zertifizierten Tools verschlüsselte Nachricht gilt als unverschlüsselt. Die Tests sind recht langwierig, darum waren bei Redaktionsschluss noch

nicht alle hier betrachteten Token FIPS-zertifiziert. Hinzugenommen haben wir den Titan Key von Google, weil dieser Konzern FIDO2 mit aus der Taufe gehoben hat.

So kamen in die Redaktion:

- ePass FIDO NFC K9, ein USB-A- und NFC-Token von Feitian Technologies;
- zwei Titan Security Keys von Google für USB-A- respektive USB-C-Ports sowie jeweils NFC;
- SafeNet eToken FIDO von Thales;
- YubiKey 5C und 5Ci FIPS für USB-A und USB-C von Yubico.

Alle Keys bestehen aus einem ABS-Polycarbonat-Gehäude und einem Metallstecker. Keinem der Produkte lag mehr als eine Kurzanleitung bei – Manuals müssen die Anwender wie heute üblich von der Hersteller-Site herunterladen, Google bietet auch das nicht. Getestet wurden die Token an einem Windows-10- und einem Windows-11-Laptop mit Edge sowie einem Mac Mini unter macOS Catalina und Chrome, also sowohl aktueller Hard- und Software als auch Legacy-Equipment. Als Gegenstelle dienten Micosofts Azure-Cloud, ein Google-Konto, der WebAuth-Testserver webauthn.io, GitHub und eine Synology-NAS-Station DS220+ unter DSM 7.1.

Folgenlos Benutzername und Passwort vergessen

Microsoft Azure bietet ein passwortloses Log-in mit FIDO2-Schlüsseln an, dito die Testsite webauthn.io. Passwortlos bedeutet dabei nicht „ohne weiteres Zutun“. Wenn der USB-Key im Slot steckt, muss der Anmeldeprozess durch eine PIN sowie eine Berührung freigegeben werden. Allerdings muss man sich nicht mehr den Benutzernamen merken, es reicht ein Mausklick auf „Mit Sicherheitsschlüssel anmelden“. Registrieren kann man ein Securitytoken – sowie andere Verifizierungsoptionen – in den persönlichen Sicherheitseinstellungen der MS-Azure-Cloud.

Der Ablauf stellt sich bei webauthn.io ähnlich dar. Bei GitHub und der Synology DS220+ kamen die Token als weiterer Faktor für eine Zwei-Faktor-Authentifizierung zum Einsatz, ebenso für das Google-Konto. Denn der Mitschöpfer von FIDO2 unterstützt zurzeit passwortloses Log-in nur mit der Google-App auf dem Smartphone, nicht mit Token.

Feitian ePass FIDO NFC K9

Ein Key für alle Zwecke: Feitians ePass FIDO NFC K9 kann auch PIV-Chipkarten ersetzen und PGP-Schlüssel aufbewahren (Abb. 1). *FEITIAN Technologies Co., Ltd.*
Das nach FIPS 140-2 und -3 zertifizierte ePass FIDO NFC K9 von Feitian braucht ebenso wie die anderen Kandidaten keine Treiber, es spielte ohne weiteres Zutun mit allen getesteten Gegenstellen zusammen. Laut Herstellerwerbung sind unendlich viele Schlüssel speicherbar, in einer Online-FAQ ist etwas realistischer von 128 Schlüsseln die Rede. Ein Sensor dient der Bestätigung durch einfache Berührung, es wird kein Fingerabdruck verifiziert. Diese Fähigkeit beherrschen nur die Feitian-Token mit dem Kürzel „Biopass“ im Produktnamen.

Feitian stellt für die weitere Konfiguration des Tokens seinen SK Manager für macOS und Windows zum Download zur Verfügung. Der SK Manager bietet Interfaces zu weiteren Securityprotokollen. So ermöglicht ein Smartcard-Modus Zugang zu Diensten, die eine PIV-Chipkarte (Personal Identification Verification) mit eigener PIN-Sicherung erfordern. Zudem lässt sich ein PGP-Schlüsselpaar auf dem Token speichern und auch wahlweise dort generieren, ebenso CERT-Zertifikate und in Verbindung mit dem SK Manager Einmalpasswörter.

Google Titan USB-A-Token

Formfaktor wie das Feitian-Token, aber völlig andere Firmware: Google Titan USB-A (Abb. 2). *Google Ireland Limited*

Das Google-Token ist vom Feitian-Key äußerlich nur durch Farbe und Aufdruck zu unterscheiden, arbeitet aber mit einer gänzlich anderen Firmware. Es funktionierte erwartungsgemäß problemlos mit Google, ebenso als zweiter Faktor gegenüber Synology, GitHub und webauthn.io. Nur die Microsoft-Cloud mochte es nicht akzeptieren – die Google-Token stehen schließlich auch nicht auf der Redmonder Kompatibilitätsliste. Zur Kompatibilität verweist Google auf FIDO CTAP1, den Standard, der die Kommunikation zwischen Browser und Authenticator definiert, und die „fehlende U2F-Unterstützung“ von Microsoft. Hintergrund: Das Titan-Token unterstützt FIDO und U2F, jedoch nicht FIDO2, und die Microsoft-Site ist nicht abwärtskompatibel zu U2F.

Thales SafeNet eToken FIDO

Sensitive Schlüsselringöse: Thales SafeNet eToken FIDO (Abb. 3). *Thales*

Von der deutschen Dependance der in Frankreich ansässigen Thales-Gruppe erhielten wir ein Demo-Kit ihrer Securitytools, ausprobiert haben wir das SafeNet eToken FIDO mit USB-A-Stecker. Dieses Token verfügt über einen als Öse für ein Schlüsselbund ausgebildeten Touchsensor. Es arbeitete ohne

weiteres Zutun mit allen Gegenstellen zusammen. Das Token kann laut Hersteller bis zu acht FIDO-Schlüssel verwalten. Eine zusammenhängende Anleitung war auf der Herstellerwebsite nicht zu finden, man muss sich die Informationen abschnittweise zusammensuchen.

YubiKey 5Ci FIPS

Mit USB-C- und Lightning-Anschluss: YubiKey 5CI FIPS (Abb. 4). *Yubico*

Vom in Schweden gegründeten und mittlerweile in Kalifornien ansässigen Sicherheitsspezialisten Yubico erhielten wir den YubiKey 5Ci FIPS, ein Token mit USB-C- und Lightning-Anschluss und – wie der Name nahelegt – mit FIPS-140-2-Validierung. Bei Registrierung und Log-in macht ein dezentes Blinken einer grünen LED des seitlich angebrachten Touchsensors darauf aufmerksam, dass eine Aktion erwartet wird.

Das Token funktionierte mit allen getesteten Gegenstellen, zudem ist es für eine Vielzahl von Protokollen einsetzbar, die sich mit dem Programm Yubi Authenticator auf Windows-, macOS- und Linux-PCs sowie unter Android und iOS konfigurieren lassen. Darüber kann man zum Beispiel eine PIV-Chipkarte ersetzen und OpenPGP-Schlüssel verwalten. Laut Hersteller passen Informationen für 32 Gegenstellen auf das Token. Ein umfangreiches englischsprachiges Online-Manual erklärt ausführlich alle Optionen. (js@ix.de)

Daten und Preise				
Produkt	Feitian ePass FIDO NFC K9	Google Titan USB-A-Token	Thales SafeNet eToken FIDO USB-A	YubiKey 5Ci FIPS
Anbieter	FEITIAN Technologies Co., Ltd.	Google Ltd.	Thales Group	Yubico
Web	ftsafe.com	google.com	thalesgroup.com	yubico.com
Maße (mm)	43,9 × 20,8 × 3,1	43,9 × 20,8 × 3,1	40 × 16 × 10	45 × 18 × 3,3
Gewicht (g)	6	6	6	10
Einzelpreis (inkl. MwSt.)	34,90 €	34,90 €	53,02 €	83,30 €

1. Quellen
2. Verweise auf die erwähnten Kompatibilitätslisten unter ix.de/zm8b