

FIDO2 tokens

- Achtergrond
- Ondersteunde browsers
- Ondersteunde FIDO tokens
 - Feitian
 - Google
 - Solokeys (pending)
 - Yubikey
 - Token 2



Sommige desktop applicaties, zoals de Microsoft Office desktop of mobile applicatie en de Mac OSX Calender en Mail werken met een ingebouwde browser die de FIDO/webauthn standaard (nog) niet ondersteunt. De login met een FIDO token werkt dan ook niet voor deze applicaties.

Achtergrond

FIDO is een technologie waarmee veilig kan worden ingelogd op websites met een authenticator. Zo'n authenticator kan een USB token zijn, maar ook een mobiele telefoon of iets wat is ingebouwd in een laptop en wat kan worden gebruikt via bij voorbeeld gezichtsherkenning of een vingerafdrukscanner). Sommige authenticators zijn geschikt voor gebruik in 2-factor authenticatie. Deze tokens worden dan ook ondersteund in SURFsecureID. Lees het [blog "Veilig inloggen voor iedereen"](#) voor meer achtergrond over FIDO2.

Voor gebruik in SURFsecureID worden de volgende eisen gesteld aan authenticators:

- Het moet echt om een 2e factor gaan, d.w.z. iets anders dan een "wat-je-weet" factor zoals een wachtwoord. Omdat FIDO gebruik maakt van public key cryptografie betekent dit dat de authenticator moet beschikken over speciale hardware om de gegenereerde private keys te beschermen. Met die speciale hardware (cryptografische chips) wordt het extreem moeilijk gemaakt de private keys uit te lezen. Als zo'n private key kan worden uitgelezen kan namelijk een kopie worden gemaakt van de authenticator, en daarmee vervalt de authenticator van een "wat-je-hebt" factor tot een "wat-je-weet" factor. Er is dan dus ook geen sprake meer van 2-factor authenticatie.
- Bij het registreren van FIDO authenticators als 2e factor controleert SURFsecureID welk type authenticator wordt gebruikt. Dat gaat op basis van een *attestation certificaat* dat door de fabrikant is ingeprogrammeerd in de authenticator. Op basis van dat attestation certificaat bepaalt SURFsecureID om welk type authenticator het gaat en of die geschikt is om private keys te beschermen met cryptografische hardware.
- Er verschijnen voortdurend nieuwe FIDO authenticators op de markt. SURF beoordeelt die producten, en beheert een allow-list van goedgekeurde FIDO authenticators in SURFsecureID. Het kan voorkomen dat nieuwe producten nog niet geëvalueerd zijn door SURF. In zo'n geval kan contact worden opgenomen met support@surfconext.nl.

Kort samengevat worden FIDO authenticators ondersteund door SURFsecureID als aan de volgende voorwaarden wordt voldaan:

1. De FIDO authenticator voldoet aan de FIDO standaard (FIDO/U2F of FIDO2/CTAP).
2. De FIDO authenticator beschikt over een attestation certificaat van de fabrikant waarmee het type authenticator kan worden bepaald.
3. De FIDO authenticator maakt gebruik van cryptografische hardware om private keys te beschermen.
4. De FIDO authenticator is [FIDO certified](#).

Ondersteunde browsers

Om met een FIDO2 token te kunnen werken moet de browser van de gebruiker de "Webauthn" standaard ondersteunen. Moderne browsers ondersteunen dit, maar oudere browsers niet. Onderstaand figuur geeft een overzicht van de browser versies die Webauthn ondersteunen:

Chrome	Edge *	Safari	Firefox	Opera	IE	Chrome for Android	Safari on iOS *	Samsung Internet	Opera Mini *	Opera Mobile *	UC Browser for Android	Android Browser *	Firefox for Android	QQ Browser	Baidu Browser	KaiOS Browser
							3.2-13.1									
							13.2									
							13.3-13.7									
							14.4	4-16.0								
							14.5-17.1	17.0-22		12-12.1		2.1-4.4.4				2.5
						120	17.2	23	all	73	15.5	120	119	13.1	13.18	3.1
4-66	13-17	12.1	60-113	10-53	6-10											
67-119	18-119	13-17.1	14-120	54-105												
120	120	17.2	121	106	11											
121-123	121	17.3-TP	22-124				17.3									

Bron en voor meer details: <https://caniuse.com/?search=webauthn>

Zie ook dit [overzicht van Yubico](#).

Ondersteunde FIDO tokens

SURFsecureID ondersteunt het gebruik van FIDO tokens (ook authenticators of security keys genoemd). Zowel FIDO U2F als FIDO2 tokens kunnen hierbij als 2e factor worden gebruikt.

De FIDO protocollen zijn gestandaardiseerd, waardoor tokens van verschillende fabrikanten gebruikt kunnen worden. Zie hieronder voor de FIDO tokens die nu ondersteund worden. Als een ander FIDO token aan de hierboven genoemde eisen voldoet kan deze toegestaan worden voor gebruik in SURFsecureID. Neem dan contact op met support@surfconext.nl.

Feitian

De volgende type Feitian-tokens zijn geschikt voor FIDO met SURFsecureID.

- MultiPass FIDO (K25)
- ePass FIDO2 (A48) en ePass FIDO2 NFC (K9)
- BioPass FIDO2 (K26 en K27)
- AllinPass FIDO2 (K27) en AllinPass FIDO2 Plus

Zie [de website van Feitian](#) voor een overzicht van de verschillende FIDO tokens.

[blocked URL](#)

Instellingen in het hoger onderwijs en onderzoek kunnen Feitian tokens met korting kopen bij de officiële resellers voor Feitian in Nederland:

- Novaris. U kunt contact opnemen met Ron Oosterwijk via ron@fidosecurity.nl of via <https://fidosecurity.nl/>.
- SYNTYCHE BV. U kunt contact opnemen met David John Rakers via david.rakers@syntyche.eu of via <https://syntyche.eu/authenticatie/>.

Google

De volgende type Google-tokens zijn geschikt voor FIDO met SURFsecureID:

- Titan Security Key (alle versies).

De Titan Key van Google is momenteel niet verkrijgbaar in Nederland

Solokeys (pending)

De volgende type [Solokeys](#) zijn momenteel in onderzoek om toegevoegd te kunnen worden in SURFsecureID:

- Solo
- Solo Tap
- Somu

NB: de Solo Hacker zal niet ondersteund worden

Yubikey

De volgende type YubiKey-tokens zijn geschikt voor FIDO met SURFsecureID.

- YubiKey 5 (FIDO2). Verkrijgbaar in verschillende vormen (USB-A met NFC, USB-C, nano, 5Ci)
- Yubikey FIPS (FIDO U2F). Verkrijgbaar in verschillende vormen (nano, USB-A, USB-C).
- YubiKey 4 (FIDO U2F). Verkrijgbaar in verschillende vormen (nano, USB-A, USB-C). Niet meer in productie.
- YubiKey Neo (FIDO U2F, RFID en NFC compliant). Niet meer in productie.
- YubiKey Edge (FIDO U2F compliant). Niet meer in productie.
- Yubico Security Key Series (de "blauwe sleutels").
 - Behalve de variant die "FIDO U2F Security Key" heet. Niet meer in productie.

Zie [de website van Yubico](#) voor een overzicht van de verschillende YubiKeys. Mocht je niet weten welke Yubikey je hebt, dan kun je dit hier [op de website van Yubico](#) nagaan.

5	4	Neo	Security Keys
			

Instellingen kunnen Yubikeys op verschillende plekken kopen. Geadviseerd wordt om dit bij [officiële Yubico resellers](#) te doen.

Token 2

De [FIDO2 sleutels van Token 2](#) kunnen ook gebruikt worden voor SURFsecureID