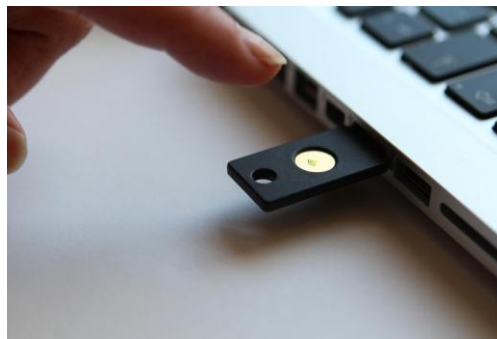


	YubiKey NEO	
	OTP-token voor sterke mobiele authenticatie	
	Systeemvereisten: USB- of NFC-interface; Platform- en browser-onafhankelijk, geen client software vereist.	
	Ontwikkeld door:	Yubico (http://www.yubico.com)
Premium token + gratis software	Contactpersoon:	bert.vanhilst@smals.be

Functionaliteiten

De YubiKey NEO is een authenticatie-token die toelaat om éénmalige wachtwoorden (OTP's - One Time Passwords) te genereren. Een OTP kan dan automatisch getransfereerd worden via zowel een **USB- als NFC-interface** (Near Field Communication). Daarom kan de YubiKey gezien worden als een gebruiksvriendelijker alternatief voor de klassieke OTP-tokens waarbij de OTP van een schermje wordt afgelezen en manueel moet overgetypt worden.

Bij het gebruik van de NFC-interface wordt standaard een URL geopend in de browser waarbij de OTP als parameter meegegeven is. Maar de NFC-tag kan ook onderschept en afgehandeld worden door een specifieke app op een NFC-toestel.



De YubiKey NEO kan gebruikt worden met password managers zoals LastPass om de toegang tot deze gevoelige gegevens (paswoordkluis) extra te beschermen.

Naast de OTP-mode is er ook een **Challenge-Response** mode, een **OATH** mode en een **Static Password** mode. Die laatste mode kan gebruikt worden om een eenvoudig te onthouden paswoord aan te vullen met een complex paswoordgedeelte dat bijgehouden wordt op de YubiKey.

De gratis **Personalization Tool** voor Windows, Linux en OS X laat toe om YubiKeys te configureren in de verschillende modes. Zo kan er een statisch paswoord geconfigureerd worden of de URL in de NFC NDEF-tag.

Voor de **validatie van OTP's** is er de keuze tussen de YubiCloud Online Validation Service of een onsite Yubico Validation Server. De gratis YubiRADIUS Virtual Appliance laat toe om de YubiKey te gebruiken voor remote access (VPN-toegang): er is integratie met bestaande AD/LDAP services, automatische koppeling tussen gebruiker en YubiKey en de software werkt samen met VPN-oplossingen als die van Juniper en Cisco.

Conclusies en Aanbevelingen

De YubiKey NEO biedt sterke authenticatie op een groot aantal toestellen, hetzij via USB-interface hetzij via NFC op NFC-compatibele toestellen. Voor een eindgebruiker is het heel gebruiksvriendelijk aangezien de OTP niet manueel moet overgetypt worden. Hardwarematig is de YubiKey NEO licht en stevig en bevat bovendien geen batterij. Enig minpunt is dat het gebruik ervan op iPad/iPhone omslachtig is (geen NFC of USB). Los daarvan kan de YubiKey NEO een gebruiksvriendelijk alternatief zijn voor de klassieke OTP-tokens.

Testen en Resultaten

De YubiKey werd getest via zowel de USB- als de NFC-interface.

- Voor het gebruik van de YubiKey via **USB** volstaat het om de YubiKey op een USB-poort aan te sluiten. De eerste maal wordt de YubiKey herkend als toetsenbord en kunnen we bijna ogenblikkelijk aan de slag zonder extra software te moeten installeren. Het invullen van een OTP in een inlog-formulier is heel eenvoudig. Het volstaat om op de knop van de Yubikey te duwen. Op dat moment wordt er een OTP gegenereerd die automatisch ingevuld wordt in het geselecteerde OTP-inputveld en wordt er automatisch een "enter" ingegeven zodat het inlogformulier gesubmit wordt. Het is dus niet meer nodig om de OTP over te typen. Dit werd succesvol getest op toestellen met Windows 7 en Windows 8.
- De YubiKey werd ook getest op een toestel met **NFC** (de HTC One X met Android 4.1). Ook hier is het niet nodig om extra client software te installeren. Wel werd de YubiKey geprogrammeerd om de OTP als parameter toe te voegen aan een specifieke URL. Voor het doel van deze testen werd een test-webapplicatie voorzien. Het herprogrammeren van de YubiKey kan met de gratis Personalization Tool van Yubico. Ook bij NFC is het gebruiksgemak groot: als de YubiKey tegen de smartphone gehouden wordt, wordt de bovenstaande URL automatisch geopend in de browser en wordt de OTP vanzelf ingevuld. Dan moet enkel nog het (statisch) paswoord ingegeven worden.



De YubiKey kan dus zonder veel moeite gebruikt worden op een groot aantal toestellen: Windows, Linux, OS X en NFC-compatibele toestellen. De YubiKey werkt ook op de iPad, maar aangezien daar geen USB-slot voorhanden is moet er gebruik gemaakt worden van de Apple Camera Connection Kit. Dat maakt het wat omslachtig en minder gebruiksvriendelijk.

Voor de veiligheid wordt een OTP best gecombineerd met een (statisch) paswoord en een gebruikersnaam. Strikt genomen is een gebruikersnaam niet noodzakelijk omdat de ID van de YubiKey vervat zit in de OTP die door de YubiKey gegenereerd wordt. Het formaat van de gegenereerde characterstring ziet er als volgt uit:

<u>vvhbhdhducjkd</u>	<u>itvdiuvudheukjeldnnjenlfuufnvbrv</u>
ID (12 chars)	OTP (32 chars)

Gebruiksvoorwaarden

Een YubiKey NEO kost momenteel €49,95 (<http://www.yubikeyshop.nl/>). De standaard YubiKey (zonder NFC, enkel USB) kost €19,95 per stuk. De Personalization Tool en de server software (YubiRADIUS, Validation Server) zijn gratis beschikbaar. De basis YubiCloud service is gratis. De premium versie (\$3 per YubiKey user per jaar) biedt een uptime SLA en reporting features. Er is ook een betalende support service beschikbaar (YubiSupport) aan \$2500/jaar. Die biedt toegang tot de technische expertise en ondersteuning van Yubico. Meer informatie over de kosten kan gevonden worden op <http://www.yubico.com/products/comparison/cost/>.