



Er heeft een kentering plaatsgevonden voor wat betreft het gebruik van onze IT-voorzieningen. Daarmee bedoelen we dat steeds minder gebruik maken van onze oude bekende "werkplek" en meer gebruik zijn gaan maken van allerlei mogelijkheden om vanaf afstand en/of mobiel te werken. Het gebruik van webapplicaties zoals bijvoorbeeld Office 365 en Google Docs is daardoor sterk toegenomen. Bedrijfsgegevens worden door gebruikers opgeslagen op "vreemde" servers die alleen via Internet bereikbaar zijn. Menig IT-manager heeft weleens twijfels over de security daarvan. De toegang tot bedrijfsgegevens, webapplicaties en cloud storage wordt verkregen met alleen user-ID en wachtwoord en is vaak zeer onveilig.

Om dergelijke toepassingen en systemen veiliger te maken, biedt ECsys het EToken Two Factor Authenticatie Platform. Naast het invoeren van alleen een user-ID en wachtwoord moet men een extra token invoeren dat gegenereerd wordt het EToken 2FA platform. Het token kunt u aanmaken via een webbrowser, 2FA app op uw smartphone (Android, Apple en Windows), Google authenticator, SMS bericht of een hardware Token.



Het EToken 2FA platform is een eenvoudig te beheren systeem waarop alle toepassingen draaien voor de benodigde authenticatie. De configuratie en het beheer van het EToken platform vindt plaats via een webinterface, die tevens voor iedere gebruiker een QR-code pagina biedt zodat het configureren van smartphones met authenticatie apps snel en probleemloos verloopt.

Office 365

De toegang tot Office 365 is net zoals bij vele andere cloud toepassingen eenvoudig beveiligd met een user-ID en wachtwoord. Ook Office 365 kan beveiligd worden met het EToken authenticatie platform. Hiervoor dient men wel gebruik te maken van een ADFS server en proxy. Ook andere Microsoft toepassingen zoals SharePoint, Lync en Outlook webaccess zijn "ADFS Claims aware" en kunnen beveiligd worden met behulp van het EToken authenticatie platform.



Remote Desktop access

Desktop omgeving worden vaak beschikbaar gemaakt via concepten zoals Citrix XenDesktop, Citrix Netscaler, Windows Terminal- of Remote Desktop Server en andere remote desktop systemen. Het EToken platform ondersteunt veel remote desktop concepten zodat verschillende authenticatie methodes toegepast kunnen worden voor de toegang tot deze desktops.

VPN verbindingen

VPN verbindingen worden toegepast om devices te koppelen aan het bedrijfsnetwerk. Dit wordt vaak gerealiseerd met alleen user-ID en wachtwoord. Het verdient de aanbeveling om een VPN-verbinding te beveiligen met Two Factor Authenticatie. Veel apparatuur biedt deze mogelijkheid via LDAP, AD en Radius.



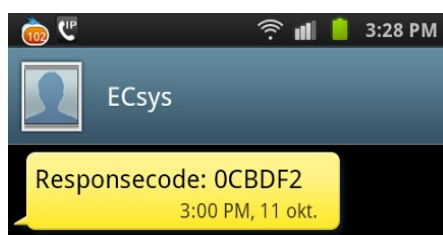
Smartphone met authenticatie applicatie

Er zijn verschillende gratis apps verkrijgbaar voor zowel Android, iPhone en Windows Mobile. Ook zijn er apps voor Palm OS, Java. De gegevens die nodig zijn om deze apps in te stellen worden verkregen via de webinterface van het EToken platform.



Google Authenticator

Google authenticator is voor het authenticeren bij verschillende websites en webapplicaties. Verschillende providers van webbased applicaties authenticeren hiermee en kunnen dit ook realiseren met de ECToken. Voorbeelden zijn; Amazon web services, Bitcoin, Dropbox, Drupal, Evernote, Google Apps en Salesforce.com. De configuratie van Google authenticator vindt plaats via een QR-code die op de webinterface te vinden is en via mail of op papier naar een gebruikers kan worden verzonden.



SMS Passcode

Na het invoeren van een user-ID en wachtwoord kan men sommige systemen zo configureren dat er naar een volgende inlog pagina gegaan wordt waar men een token moet invoeren. In een dergelijk geval kan men dit token toesturen via een SMS bericht naar de mobiele telefoon van de gebruiker zodat deze zich kan authenticeren. Echter moet bij sommige systemen (bijv. Citrix) user-ID, wachtwoord en passcode tegelijkertijd worden ingevoerd. In zo'n geval kan men niet werken met SMS tokens.

Hardware token

Hiermee bedoelen wij de overbekende token calculatoren zoals die al sinds lange tijd worden toegepast. Wanneer men in het bezit is van dergelijke hardware tokens (OAUTH) kan men deze blijven gebruiken.

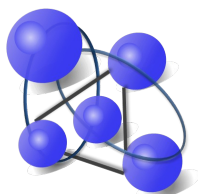


YubiKey

Sommige organisaties gebruiken Yubikey's voor het authenticeren. Het ECToken platform heeft een plug-in zodat men ook met behulp van deze Yubikey's kan authenticeren.

Virtueel of Fysiek geïnstalleerd

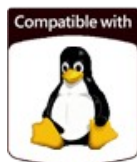
U mag kiezen hoe u het ECToken Authenticatie Platform wilt hebben. We kunnen het fysiek geïnstalleerd op een server systeem leveren of als een image voor een Virtualisatie platform. Hierbij hanteren wij VM-ware, Citrix XEN-server, XEN (oss) en Hyper-V.



Supported Authenticatie Interfaces

Het ECToken 2FA platform support de volgende Interfaces:

- Radius based authenticatie
- SAML2 based authenticatie
- ADFS Claim based authenticatie (voor Microsoft Cloud toepassingen)



Linux en Open Source Solutions
Eekhoornbos 19
3892 WP Zeewolde
T: 085 2100225
www.ecsys.nl