Tokenløsning til sikker adgang

En tokenløsning giver sikker adgang til at afvikle et Fjernskrivebord for en bruger uanset hvor denne befinder sig.

Eneste krav til brugernes eksisterende udstyr er, at det er i stand til at afvikle en browser med enten ActiveX- eller Java-understøttelse. Alle moderne browsere til alle platforme er i stand til dette, hvorfor både Windows-, Mac- og Linux-brugere vil kunne tilkoble sig.
Vores løsning anvender en såkaldt token, som er et lille stykke hardware, der f.eks. kan placeres i brugerens nøglering. Denne token har én funktion, nemlig at generere éngangskoder, hvilket sker ved at brugeren trykker på en knap, hvorefter en 6-cifret kode kortvarigt vises i display'et.

Token til generering af éngangskoder

Funktionen og sikkerheden er tilsvarende den, der anvendes af f.eks. bankerne i form af NemID – vores token er blot baseret på et lille stykke hardware frem for et papkort.

Princippet for at tilgå løsningen er følgende (se korresponderende skærmbilleder på side 3):

1) Brugeren åbner en browser og kobler via en SSL-krypteret hjemmeside op til en VPN-server.
   Her mødes brugeren med krav om brugernavn, password og éngangskode.
   Kun brugeren kender passwordet, og kun brugerens token kan generere éngangskoden.
   En anden brugers token vil ikke kunne anvendes, da de enkelte fysiske tokens og deres éngangskoder er tilknyttet de enkelte brugernavne.

2) Når brugernavn, password og éngangskode er godkendt kan brugeren fra en liste vælge den ønskede terminalserver.

3) Brugeren mødes nu af sin velkendte Windows logon-skærm.
   Windows-brugernavn og –password indtastes, og brugeren kan herefter arbejde med sine applikationer og filer på Skrivebordet.

Fionia IT ApS · Overgade 14 st · 5000 Odense C · CVR 25531205 · mail@fioniait.dk

Sikkerhedsmæssige fordele

- **Der anvendes éngangskoder**
  Herved sikres, at selvom uvedkommende skulle få kendskab til en eller begge af en brugers brugernavn/password-kombinationer er disse ikke anvendelige i sig selv.
  Selvom en uvedkommende skulle opsnappe alle tastetryk ved logon – inklusive éngangskoden - kan dette ikke efterfølgende anvendes, da der jo er tale om netop éngangskoder.

- **Der anvendes separate brugernavn- og password-kombinationer, der teknisk er uafhængige**
  Der er ikke installeret udvidelser eller andet i terminalløsningens Active Directory.

- **Brugernes maskiner er ikke netværksmæssigt i direkte kontakt med terminalserveren**
  En terminalsession, der afvikles på en brugers maskine, har udelukkende kontakt med VPN-serveren, der så videreformidler data mellem brugeren og terminalserveren via et lukket netværk.
  Mellem VPN-serveren og terminalserveren er ydermere placeret en uafhængig stealth firewall (netværksmæssigt usynlig for omgivelserne), der sikrer, at der udelukkende kan åbnes terminalsessioner fra VPN-serveren til terminalserveren.
  En bruger, der anvender en maskine inficeret med virus, er således ikke engang i stand til at forsøge at overbringe smitten til terminalserveren.

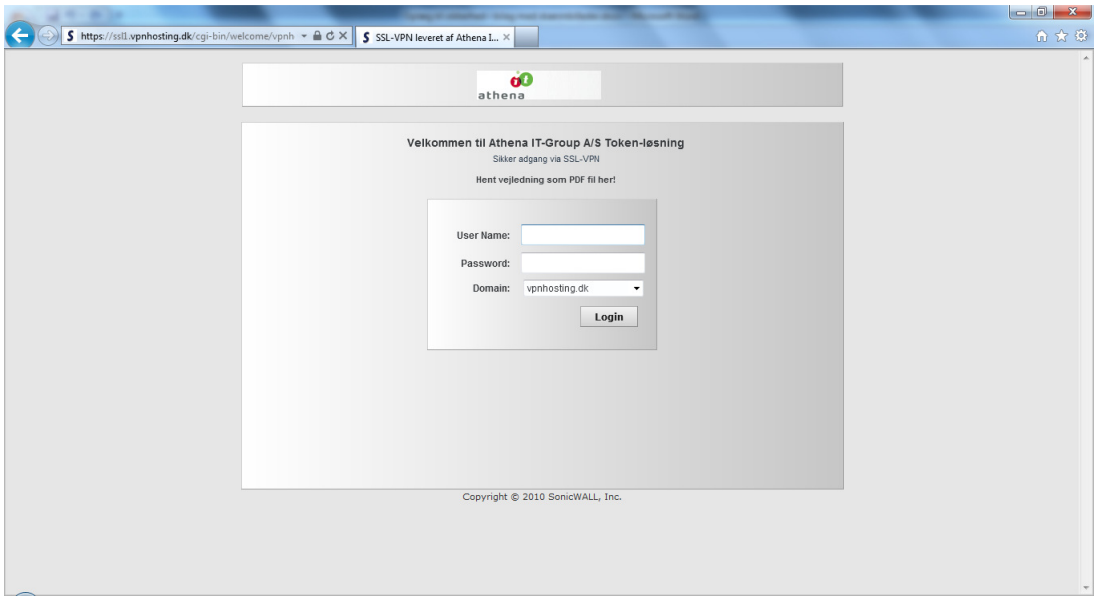
- **Der anvendes VPN via HTTPS i en browser**
  Stadig flere steder, som f.eks. lufthavne, hoteller og restauranter, lukker ned for muligheden for at brugerne via gæstenet kan etablere traditionelle VPN-forbindelser.
  Derimod tillader alle krypteret trafik i browsere.

- **Stærk kryptering**
  Den foreslåede løsning krypterer trafikken to gange – både via SSL/VPN samt det faktum, at terminalsessionen i sig selv er 128-bit krypteret.

Fionia IT ApS · Overgade 14 st · 5000 Odense C · CVR 25531205 · mail@fioniait.dk

Skærmbilleder

1) I feltet 'User Name' angives brugernavn, i feltet "Password' angives password samt 6-cifret éngangskode.



2) Brugeren kan nu klikke på den terminalserver, som han ønsker at logge på.