



ezenta
Sikre rammer om IT



BRUG DIN MOBIL SOM TOKEN - DER HAR DU NØGLEN TIL ØGET SIKKERHED!

SMS PASSCODE® er en **to-faktor sikkerhedsløsning**, hvor brugerens **mobiltelefon** anvendes som "token-enhed". Det er ikke alene smart. Det har en række **sikkerhedsmæssige fordele**. SMS PASSCODE® sætter i modsætning til de gammeldags token-løsninger en effektiv **stopper** for **Phishing** og **Pharming** angreb, og systemet **detekterer automatisk** potentielle **Brute force** samt **Denial of Service** angreb. Løsningen er **challenge-baseret**, hvilket vil sige, at den adgangsgivende **passcode** (engangskode) først sendes til brugeren, efter at brugernavn og adgangskode er valideret. Koden kan kun anvendes fra den browser-session / VPN klient hvorfra den er forespurgt, og kan derfor ikke misbruges. Løsningen er **enkel at implementere**, men **opfylder alle krav** til et enterprise it-miljø. **Sikkerhed** og **skalering** er gennemgående, og løsningen tilbyder **fail over**, **load balancing** og **kryptering** mellem alle komponenter.

På de følgende sider kan du læse mere om hvad løsningen beskytter, hvorfor den også er sikrere ud fra et brugerspekt, og hvorfor token-løsninger ikke længere er sikre nok. God læselyst.

For at være sikker på, at kun godkendte brugere opnår adgang til virksomhedens systemer, skal du fremadrettet anvende et to-faktor sikkerhedssystem som er challenge-baseret og sessions-specifikt. SMS PASSCODE® er netop et sådant system - Et nyt våben, der sætter en effektiv stopper for de aktuelle sikkerhedstrusler.

HVORDAN FUNGERER SMS PASSCODE®?

Løsningen fungerer ved, at brugeren angiver brugernavn og adgangskode på login-stedet. Derpå validerer SMS PASSCODE® om brugeren er oprettet, hvorefter brugerens adgangskode valideres (typisk i Active Directory). Kun såfremt denne er korrekt, genereres og sendes der en passcode (engangskode) til brugerens mobil-telefon. Derved er løsningen challenge-baseret.

Herpå indtaster brugeren den modtagne passcode indenfor 2 minutter (kodens levetid kan konfigureres). Den tilsendte passcode kan alene anvendes fra den browser-session/VPN klient, hvorfra den er forespurgt - altså sessions-specifikt. Såfremt passcode og sessions ID er korrekt lukkes brugeren ind.

Enklere og mere sikkert kan det ikke gøres!



HVORFOR SMS PASSCODE®?

Der er mange grunde til at vælge SMS PASSCODE®, men for de fleste kunder er målet at tøjle sikkerheden, samt at gøre livet lidt lettere for brugerne. Dertil kommer, at de fleste har ønsket at reducere de samlede omkostninger (TCO) til deres to-faktor sikkerhedsløsning.

→ Det er smart at anvende sin mobiltelefon, som man altid har med sig og som man ikke giver fra sig, da den er personlig. Og SMS teknologi er klippestabil, blandt andet pga. tele-selskabernes kommercielle interesser.

→ Et token skal registreres og distribueres til brugeren. I større virksomheder er logistikken og administrationen forbundet hermed en stor og krævende opgave. Med SMS PASSCODE® slipper man for logistikken og administrationen er minimal.

→ Tokens kan ikke længere løfte opgaven! Brugeren angiver alle oplysninger på én gang (inkl. token-kode). Hackeren kan let oprette et falsk login-site (phishing-site) og stjæle alle de nødvendige oplysninger fra brugeren.

“Så snart vi hørte om SMS PASSCODE® var vi klar over at det var løsningen for os! Vi bruger systemet til alle hjemmearbejdspladser, fordi det til fulde lever op til vore sikkerhedskrav og samtidig er en meget brugervenlig løsning.”

Hans Stockholm, IT-arkitekt, Alm. Brand.

[Alm. Brand har i 3 år benyttet SMS PASSCODE® til 1200 brugere]

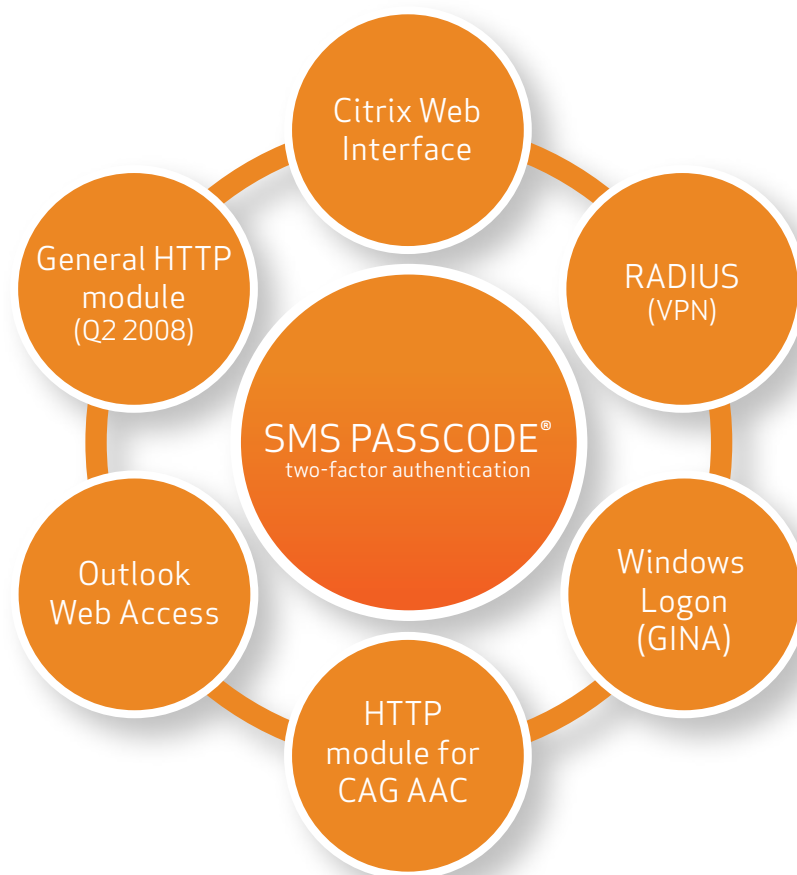
HVAD KAN BESKYTTES?

SMS PASSCODE® understøtter de mest udbredte it-systemer til ekstern adgang (remote access) og der er fuld integration til Citrix og Radius/VPN. Eksempelvis beskytter vi Citrix Web Interface og RADIUS/VPN klienter fra Checkpoint, Cisco, Citrix Access Gateway og Juniper.

Per 2008 understøttes desuden: Outlook Web Access (OWA), GINA (Windows Logon), SharePoint Portal Server og Web Sites baseret på Microsoft IIS.



Brugerne angiver, med token-løsninger, alle oplysninger på én gang (brugernavn, adgangskode og token-kode). Hackeren får alle nødvendige oplysninger til at logge på det originale login-site.



SIKKERHEDSASPEKTER

SMS PASSCODE® yder effektiv sikring imod Phishing-angreb, idet passcodes er challenge-baserede, sessions-specifikke og tidsbegrænsede. Passcodes genereres gennem et FIPS-140 godkendt modul, som sikrer kryptografisk stærkt tilfældigt genererede engangs-koder, som kan konfigureres i forhold til levetid og kompleksitet. Al netværkskommunikation er 256 bit AES krypteret i et multiserver setup.

Løsningen detekterer "Brute force" angreb, hvorved der automatisk blokeres for brugere ved gentagen anvendelse af ukorrekt passcode ligesom der blokeres automatisk ved Denial-of-service angreb.

ENTERPRISE-ASPEKTER

For at imødekomme vore kunders krav til opetid, er løsningen designet med load balancing og fail over på samtlige komponenter; modems, transmitter osv. Endvidere kan løsningen skaleres til et uendeligt antal brugere og servere. I internationale set up, placeres lokale modems typisk verden over, men forbindes til én SMS PASSCODE® løsning.

BRUGERASPEKTER

På brugersiden tegner SMS PASSCODE® sig også for væsentlige sikkerhedsforbedringer, der støtter op om store virksomheders behov for effektivisering og fleksibilitet.

- En bruger opdager hurtigt, hvis dennes mobiltelefon er stjålet eller er bortkommen. Det betyder kort responstid, hvormed et potentielt sikkerhedsbrud afværges hurtigere, end det typisk er tilfældet ved token-løsninger. Heri ligger en mærkbar forbedring af sikkerheden.
- Brugeren sørger selv for at spærre SIM-kort i tilfælde af en stjålet eller bortkommen mobiltelefon – og er endda motiveret for at gøre det, for at undgå misbrug af telefonen. Dermed blokeres adgangen til systemer, beskyttet med SMS PASSCODE® ligeledes hurtigt og effektivt.
- Selvhjulpne brugere betyder, udover den kortere responstid, en reduktion af arbejdsbyrden, der traditionelt påhviler administrator i tilfælde af sikkerhedsbrud.

SÅDAN KOMMER DU VIDERE

Vil du vide mere om SMS PASSCODE®, så kontakt:

Ezenta A/S
 Jesper Sobol
 Sales Director
 Telefon: +45 25 35 15 94
 jes@ezenta.com

