

Tunnel-kryptering

Ønsker I at forbedre arbejdsgangene ved afsendelse af mails til myndigheder og partnere?

Og ønsker I:

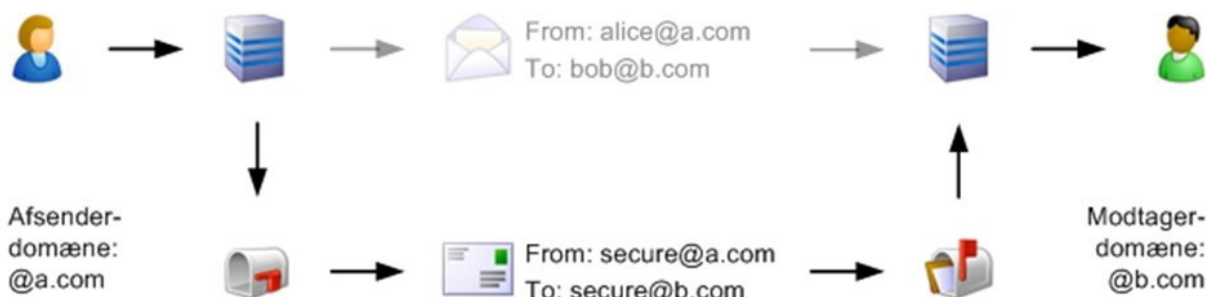
- At sende sikre mails direkte til enkeltpersoner hos en anden myndighed/partner?
- Automatisk at sikre sikkerheden ved afsendelse til udvalgte myndigheder/partnere?
- At benytte en veldefineret og standardiseret løsning?

Tunnel-kryptering (også kaldet domæne-kryptering) sikrer, at alle mails mellem to eller flere domæner automatisk bliver sendt som sikre mails.

Normalt sendes mails mellem myndigheder via afdelingspostkasser for at sikre besvarelse og anonymisering af den enkelte rådgiver. I visse tilfælde bliver dette et forsinkende mellemlid, som tunnel-kryptering råder bod på, idet der kan sendes mails direkte til enkeltpersoner uden at skulle tænke på sikkerheden ved afsendelsen.

Eksempel:

En konsulent i et jobkonsulenthus ønsker at sende fortrolige e-mails direkte til en sagsbehandler i kommunen.



1. Konsulenten udarbejder en e-mail og vedhæfter de relevante dokumenter. Modtagerens mail-adresse indtastes og e-mailen afsendes som normalt.
2. E-mailen sendes via den krypterede SSL forbindelse til Sikker Mail Service.
3. Sikker Mail Service aflæser modtagerens mailadresse - herunder domænet (i dette tilfælde b.com) og kan se, at e-mailen skal sendes krypteret til modtageren. E-mailen krypteres med modtagerens virksomhedscertifikat (i dette tilfælde kommunens) og sendes krypteret over internettet til kommunens Sikker Mail Service.
4. E-mailen dekrypteres af Sikker Mail Service, inden den videresendes via Sikker e-mail postkasse til modtagerens medarbejderpostkasse.

Yderligere detaljer

Gruppen af modtagere defineres blot ud fra domænenavnene på modtagerene (f. eks. horsens.dk), og funktionen sættes op, og aktiveres, uden at de enkelte brugere skal involveres.

For at lette opsætningen opdaterer DSI-NEXT en liste over domæner, der allerede kan modtage tunnel-mails.

Tunnel-kryptering kræver at domænerne, hver især har et certifikat og et nøglepar, der kan anvendes til formålet samt en Sikker Mail-løsning, der understøtter domænekryptering.

I domænekryptering anvendes afsenders og modtagers sikre postkasser kun som mellemstationer, der henholdsvis krypterer og dekrypterer en mail inden mailen afleveres til den endelige modtager.

Om DSI-NEXT



DSI-NEXT A/S udvikler og leverer intuitive IT-løsninger til både det private og det offentlige marked. Virksomheden er en del af JS Holding-koncernen, der beskæftiger godt 100 personer, omsætter for over 100 mio. kr. og har en egenkapital på 40 mio. kr.

Vores dedikerede Digital Signatur-afdeling har igennem snart 10 år udviklet og implementeret løsninger baseret på den offentlige digitale signatur (OCES) og Nets Danmarks NemID.

Vores kunder inden for dette område består af en lang række kommuner, regioner, styrelser samt større virksomheder inden for bl.a. pensionsbranchen og banksektoren.