

Turvallinen sanomanvälitys Internetissä – rutiiniako?

Kimmo Laine



kimmo.laine@edimaster.fi

Lemminkäisenkatu 14-18

PL 87

TURKU

www.edimaster.fi

TradeXpressin tarjoamat mahdollisuudet

EDIINT AS1

- Toteutettu SMTP –protokollalla
- S/MIME (Secure Multi-Purpose Internet Mail Extensions) OpenSSL toteutuksella
- Kuittauksien käyttö (MDN)

TradeXpressin tarjoamat mahdollisuudet

EDIINT AS2

- Toteutettu HTTP/HTTPS –protokollalla
- Kryptaus ja allekirjoitus käyttäen OpenSSL:ää
- Kuittaukset (MDN) joko synkronisesti tai asynkronisesti, lisäksi myös esim. CONTRL – sanomat
- Drummond Group sertifiointi 05/2009

TradeXpressin tarjoamat mahdollisuudet

EDIINT AS3

- Toteutettu FTP -protokollalla
- Suorat kumppaniyhteydet
- Push/Pull ?

TradeXpressin tarjoamat mahdollisuudet

Muut tietoturvalliset siirtotavat

- HTTPS
 - yleistyy nopeasti
- FTPS/EFTPS
 - harvinainen, ”palomuuriongelmallinen”
- SFTP
 - yleinen mutta ongelmallinen lukuisten client/server toteutuksien yhdistelminä

Nykytilanteen rutiinit

FTP laajalti käytössä. Turvallisuuden tunne / ”tietoturva” perustuu palomuriavauksiin, ei tiedon salaukseen.

FTP yhteys helppo/nopea toteuttaa lähes mihin tahansa, ei vaadi erityisiä toimenpiteitä eikä sovittavia asioita.

AS1 ja AS3 harvinaisia, ei missään nimessä lähelläkään rutiinia.

Nykytilanteen rutiinit

AS2 yleisty, yhteyksien tekeminen helpottuu koko ajan käyttäjien lisääntyessä. Atlantin toiselle puolelle pääsy vielä haasteellista. Lunastamassa paikkaansa hyvällä toteutuksella.

Salaus ja tunnistaminen ovat nykypäivää (esim. verkkopankit ja muu sähköinen asiointi)

Monen sisäisen jakelukanavan yhdistäminen yhdeksi ulkopuoliseksi yhteydeksi

Tulevaisuuden rutiinit

Tiedon salaaminen päästä päähän ja sen tallennus salattuna/pakattuna

Koneiden tunnistus arkipäivää

Yhä pienimuotoisemmatkin yhteydet turvallisia reittejä pitkin

Tiedonsiirron rajoitteet