Endring i bruk av krypteringsalgoritmer for asynkrone meldinger

Pålagt å gå fra SHA-1 over til SHA-256 – tidsrom 1. september til 1. januar 2022

Orientering fra NHN når det gjelder e-resept:

SHA (Secure Hash Algorithm) er en samling av kryptografiske sjekksumsfunksjoner som er designet av National Security Agency (NSA).

- SHA-1 er ikke ansett som sikker, SHA-1 er ikke anbefalt brukt til anvendelser innen sikkerhet etter 2010.
- SHA-256, SHA-512, SHA-224 og SHA-384 hører til SHA-2-familien og bruker den samme algoritmen. Forskjellen er at de har ulik størrelse på den ferdige hash-verdien (256/512 biter)..

Oppdatering vedr. innføring av SHA-256

- 1. september i år; virksomheter må ta imot meldinger med SHA-256, 1. januar 2022: virksomheter må sende meldingar med SHA-256
- RF kan allerede motta på SHA256 for asynkrone meldinger.
- RF vil registre de aktørene som sender ebXML på SHA-256, og svare på SHA-256.
    - Dette kan ved behov omgås manuelt i overgangsperioden (1.september 2021 – 1.januar 2022
- NHN vil følge overgangen fra SHA-1 til SHA-256, slik at vi har kontroll på framdrift blant aktørene.
- Uke 21 og 22 gjennomfører Seksjon Innføring 1:1 møter med leverandørene.

(Asynkrone meldinger (basert på ebXML): M6,M7, M8, M21 etc.)