



Valtiovarainministeriön kirjaamo

Aarne Hummelholm
Erityisasiantuntija

HALTIKin lausunto salausohjeen luonnoksesta

Ohessa HALTIKin kommentit lausuntopyyntöön VM047:18/2007.

Päivitetty salausohje on odotettu VAHTI ohjeistus. Yleisenä kommenttina voidaan todeta, että salausohje on hyvä yleisluontoinen dokumentti. Kappaleessa 6 on hyvin huomioitu analyysi sekä valinta perustuen mm. kryptovahvuuksiin suhteessa uhkaan ja vaikuttavuuteen (6.3.1).

Dokumenttia voisi kehittää vielä konkreettisten käytännön esimerkkien avulla. Tästä esimerkkinä mm. SSL 3.0, jonka suojausratkaisu on tunnetusti murrettu eikä näin ollen tarjoa enää luotettavaa salausta missään olosuhteissa. Tällaisten salausratkaisujen koostaminen tähän dokumenttiin tarjoaisi helpon ja nopean tavan varmistaa jo poistuneet salausratkaisut, viitaten toki siihen, että valitun salausratkaisun kelpoisuus tulee aina tapauskohtaisesti vielä erikseen arvioida.

Hallinnon tietotekniikkakeskus

Tietoturvapäällikkö Sonja Marjamäki

Asiakirja on sähköisesti allekirjoitettu asiankäsittelyjärjestelmässä. Haltik 07.05.2015 klo 11.58. Allekirjoituksen oikeellisuuden voi todentaa kirjaamosta.

