Terveydenhuollon tietojärjestelmien tietoturvan toteuttaminen: suunnittelu ja PKI"

Taustaa

Public Key Infrastructure (PKI) käännetään suomessa julkisen avaimen menetelmäksi. Tämä on joukko toimenpiteitä, ohjeita ja teknologioita, joilla toteutetaan sähköisen tiedon eheyteen (/muuttumattomuuteen), luottamuksellisuuteen ja kiistämättömyyteen tarvittavat toimenpiteet. PKI:ta voidaan pitää ainoana varteenotettavana menetelmänä taata nämä vaatimukset työ- ja hallinnollisten prosessien muuttuessa sähköisiksi.

Terveydenhuollon alalla tiedon eheyteen, luottamuksellisuuteen ja kiistämättömyyteen liittyvä tietoturva on suuren mielenkiinnon kohteena. Tähän on yhtenä syynä se, että terveydenhuollossa työ- ja hallinnolliset prosessit sähköistyvät kiivasta tahtia kasvavien tehokkuusvaatimuksien myötä kun samalla käsiteltävien aineistojen tietosuojaan ja oikeusturvaan liittyvät vaatimukset pysyvät ehdottoman kovina.

Muunmuassa jo vuonna 2001 tehdyn tutkimuksen mukaan tietotekniikka käytetään terveydenhuollossa paljon: yli 90% tutkimukseen vastanneista ilmoitti käyttävänsä tietotekniikkaa päivittäin työssään. Saman tutkimuksen mukaan eri terveydenhuollon ammattiryhmillä on kasvava tarve käyttää tietojärjestelmissä olevia yksityiskohtaisia potilastietoja. Mikäli siis jos yli 90% vastanneista käyttää informaatioteknologiaa työnsä takia ja kokee samalla tarpeen jopa käytön lisäämiselle, niin saavatko kaikki juuri sen tiedon mitä he tarvitsevat? Tietosuojaan ja oikeusturvaan liittyvän tietoturvan kannalta on myös kysyttävä tarvitsevatko kaikki kaikkea sitä tietoa mitä he saavat? Voidaanko siis puhua myös hallitusta informaation käyttöönotosta tietoturvan yhteydessä?

Tavoitteet

Kuopiossa käynnistämämme hankkeen yhtenä tavoitteena on kehittää luotettava menetelmä terveydenhuollon organisaatioiden tietoturvapolitiikkojen – suunnitelmien ja käyttöönoton toteuttamiseksi. Organisaatioiden tulee huomioida suunnittelussa, miten ja

mitä PKI:n funktioita prosessin missäkin vaiheessa tulisi käyttää, jotta PKI vastaisi niitä tarpeita joita uudet sähköiset työ- ja hallinnolliset prosessit tuovat mukanaan. Käyttöönotossa tärkeällä sijalla on henkilökunnan kolutukseen käytettävien resurssien määrän arvioiminen ja rutinoitujen tietoturvaprosessien ja -käytäntöjen kehittäminen terveydenhuollon erityistarpeisiin.

Toimenpiteet

Hankkeessamme keskitytään organisaatiokohtaisten tietoturvasuunnitelmien ja onnistuneen PKI:n käyttöönoton suunniteluun. Prosessissa hyödynnetään STAKES:n julkaisemia suosituksia. Suunnittelun ja määrittelyn työkaluina käytämme Zef Solutiosin tiedonkeruu- ja raportointi-järjestelmää, johon olemme laatineen kysymykset mm. ISO17799 standardin perusteella. Toisena työkaluna käytämme Immosen kehittämää 3D mallia, jolla pyritään selvittämään PKI funktioiden ja eri terveydenhuollon ammattilaisen roolien välistä suhdetta. PKI:n toteuttamiseen käytämme Utimacon SafeGuard teknologioita, joiden avulla toteutamme varmennepalvelut ja –järjestelmät. Käytämme SafeGuard ratkaisuja mm. varmenteiden tuottamiseen ja julkaisuun, vahvaan roolipohjaiseen tunnistukseen työ- ja verkkoasemille sekä lainvoimaisten sähköisten allekirjoitusten suorittamiseen.

Tulokset

Prosessin tuloksena tullaan esittelemään suunnittelu- ja käyttöönottomalli, jonka perusteella otetaan käyttöön WellTeknian eHealth pilotointiympäristössä Commit:n teleradiologiajärjestelmä, johon on integroitu Utimacon PKI työkaluja TEO:n varmenteella.

Aapo Immonen
WellTeknia

Teknia Oy