Loppuraportti: VOTI - Vakioitu operatiivinen työasemainfrastruktuuri TUPO - Pelastustoimen operatiivisten tietojärjestelmien tietoturvapolitiikka

Marko Hassinen
Juhani Silvennoinen
Pelastusopisto

Pelastusopiston julkaisu

B-Sarja: Tutkimusraportit

4/2014

ISBN: 978-952-5905-52-6 (pdf)

ISSN: 1795-9160

Sisällys

PELASTUSOPISTO

VOTI ja TUPO -hankkeiden loppuraportti

Vakioitu operatiivinen työasemainfrastruktuuri

Pelastustoimen operatiivisten tietojärjestelmien tietoturvapolitiikka

Hassinen Marko, FT, Pelastusopisto, Tutkimus- ja kehittämisyksikkö

Silvennoinen Juhani, Insinööri, Pelastusopisto, Tutkimus- ja kehittämisyksikkö

Tutkimusraportti 32 s., 2 liitetä (9 sivua)

Lokakuu 2014

TIIVISTELMÄ

Pelastusopiston tutkimus- ja kehittämisyksikön toteuttaman ja Palosuojelurahaston pääasiallisesti rahoittaman VOTI hankkeen tavoitteena oli määritellä vakioitu työasemakonsepti pelastustoimen käyttöön.

Vastaavasti TUPO hankkeen tavoitteena oli luoda edellytyksiä pelastustoiminnan tulevaisuuden tietojärjestelmien käyttöön tarvittavan toimintaympäristön rakentamiseen. Olennaisena osana näiden ympäristöjen rakentamista ovat tietojärjestelmien asettamien tietoturvavaatimusten tyydyttäminen.

Vaikka työn konteksti molemmissa hankkeissa oli luonnollisesti pelastustoimessa, työssä pyrittiin rakentamaan ratkaisua joka olisi kaikkien viranomaisten käytettävissä.

Hankkeiden tärkeimpinä yhteistyökumppaneina olivat pelastuslaitokset, Viestintävirasto, Erillisverkot Oy, Sunit Oy sekä Istekki Oy.

Pelastuslaitoksilta kerättiin tietoa nykyään käytössä olevista laitteista ja toimintaympäristöstä sekä vaatimuksia ja toiveita tulevaisuuden ominaisuuksista. Näiden saatujen tietojen pohjalta lähdettiin rakentamaan kokonaisuutta joka tarjoaa pelastustoimelle operatiivisen työaseman, tietoliikenteen, tietoturvan ja tämän konseptin päällä käytettävät pelastustoimea tukevat ohjelmat sekä tätä kokonaisuutta tukevan palvelinympäristön.

Hankkeessa itselleen asettamana tavoitteena oli ensimmäisen vuoden aikana tuottaa ST IV tason tietoturva vaatimukset täyttävä kohtuuhintainen työasemavakiointi ja pilotoida tämä. Tämän määrittelytyön ollessa jo käynnissä ilmeni, että TUVE-verkon käyttöönoton myötä vakiointi ja tietoturvamääritykset tulevat KUNTU-hankkeesta jolloin VOTI ja TUPO hankkeiden fokus siirrettiin vakioinnin päälle tuotettaviin palveluihin ja niiden kehittämiseen. Samalla laadittiin toimintasuunnitelma (Pelastustoimen tietoturvastrategia 2017) jolla seuraavan kolmen vuoden aikana pelastustoimi pääsee turvallisuusviranomaisten yhteisten tietojärjestelmien käyttöön riittävälle tietoturvallisuuden tasolle.

EMERGENCY SERVICES COLLEGE

Standardized Operative Workstation Infrastructure for Fire and Rescue Services

Data Security Policy for Operative Fire and Rescue Data Systems

Hassinen Marko, Ph.D., Emergency Services College, R&D unit

Silvennoinen Juhani, B.Eng., Emergency Services College, R&D unit

Research report 32 pages, 2 attachments (9 pages)

October 2014

ABSTRACT

TUPO and VOTI were a projects lead by the R&D unit of the Emergency Services College, Finland. These projects were funded mostly by the Fire Protection Fund (Palosuojelurahasto). Most important partners in the project were the Finnish network operator Erillisverkot Oy, Finnish Communications Regulatory Authority (Ficora), Sunit Oy, Istekki Oy, and the network of Finnish fire departments.

In order to specify the concept of the operational workstation infrastructure, a study of the existing ICT equipment, applications and services used was made. Also, the future expectations regarding operative computing environment were surveyed. Based on the information gathered, an operative workstation that provides applications, communication technology and adequate data security was defined. Facilitated by this workstation concept, applications and server functionality that fire & rescue needs, were defined.

In the TUPO project, main goal was to prepare the Fire & Rescue organizations for the future provision of common data systems for all safety and security officials. To meet this goal, a lot of work remains to be done in terms of data security. The project initiated this work by preparing guidelines and a strategy that will take the Fire & Rescue organizations to the required data security level in the near future. Certainly, this requires investment in the form of resources and effort within the next three years.

Johdanto

Pelastustoimen tietojenkäsittely-ympäristö on muuttumassa vauhdilla, jollaista aiemmin ei ole koettu. Uusien tietojärjestelmien myötä paineita tulee sekä työprosessien muutokseen, että erityisesti työ-ympäristön muuttumiseen. Pelastustoimi on aiemmin toiminut ICT ympäristönsä osalta varsin autonomisena ja muista viranomaisista erillään kuntatoimijana joka on itsenäisesti voinut tehdä päätöksiä ja linjavetoja tietojenkäsittelyn toimintatavoista ja välineistöstä. Päätöksenteko on ollut kuntasektorille ominaisesti hyvin autonomista ja pelastuslaitoksittain ollaan päädytty usein verraten erilaisiin toimintatapoihin.

Turvallisuusviranomaisille yhteiset tietojärjestelmät, kuten ERICA ja KEJO luovat tarpeen pelastustoimelle näyttäytyä yhtenä viranomaistahona, nykyisen 22 tahon sijaan. Jotta olennainen hyöty tulevista järjestelmistä saadaan käyttöön, tulee pelastustoimella olla selkeitä, toimialalle yhteisiä tavoitteita, toimintamalleja ja linjauksia joiden mukaan pelastustoimi esiintyy muiden viranomaisten suuntaan.

VOTI ja TUPO hankkeet ovat lähtökohdiltaan tähdänneet toimiin, joilla edellä kuvattua yhtenäisyyttä voidaan tuoda pelastustoimeen. Hankkeiden tavoitteena on ollut kehittää koko maan pelastustoimen ICT työtä tukevaa materiaalia, tutkittua tietoa, parhaita käytänteitä ja konkreettisia ympäristöjä. Hankkeiden perustavoite on ollut mahdollistaa pelastustoimen menestyminen tulevaisuuden yhtenevässä turvallisuusviranomaisten toimintaympäristössä.

Liitynnät muihin hankkeisiin ja toimintaympäristöön

Toimintaympäristö

Hankkeiden käytännön suunnitteluun ja toteutukseen vaikuttivat useat käynnissä olevat ja hankkeen aikana käynnistyneet pelastustoimea koskevat IT hankkeet, sekä jo olemassa oleva infrastruktuuri. Tässä kappaleessa käsitellään näitä hankkeita ja ympäristöä hyvin tiivistetyssä muodossa. Kaikista näistä hankkeista ja ympäristöistä löytyy kattavia esityksiä joita ei ole nähty järkeväksi toistaa tässä raportissa vaan lähinnä tuoda esiin niitä erityispiirteitä jotka vaikuttavat langattoman laajakaistan määrittelyyn. Samalla kuvataan hankkeiden välistä vuorovaikutusta ja käytännön toimenpiteitä.

PEIP

Pelastustoimen IP verkko (PEIP) on Erillisverkot Oy:n pelastuslaitoksille tuottama palvelu, joka on toteutettu olemassa olevalla verkkoinfrastruktuurilla MPLS (Multiprotocol Label Switching) verkkona. Verkko yhdistää pelastuslaitokset ja mahdollistaa pelastuslaitosten yhteisten palveluiden tuottamisen keskitetyssä, pelastustoimen hallinnoimassa verkkoympäristössä. PEIP verkkoa kehitetään edelleen pelastuslaitosten tietoliikenneverkkoprojektissa tavoitteena mm. yhteisten tietoverkkopalvelujen (mm- pääsynhallinta ja videoneuvottelu) tuotteistaminen. VOTI hankkeen pilotissa tietoliikenne pyrittiin lähtökohtaisesti rakentamaan ajoneuvosta suoraan PEIP verkkoon. Tämä tavoite jäi kuitenkin saavuttamatta. Onnistuakseen tähän olisi tarvittu Erillisverkot Oy:n LIP (Liikkuva IP) palvelu, jonka otto tuotantokäyttöön on viivästynyt. VOTI pilotissa on kuitenkin täysi valmius siirtyä LIP palvelun käyttöön heti kun palvelu on tuotannossa.

ERICA

Uudeksi hätäkeskustietojärjestelmäksi hätäkeskuslaitoksen sivuilla kuvattu ERICA tullee muuttamaan myös pelastustoimen useita prosesseja. Lyhenne tulee sanoista E = Emergency, R = Response, I = Integrated, C = Common, A = Authorities, mikä viestii kyseessä olevan viranomaisten yhteinen tietojärjestelmä. (http://www.112.fi/hatakeskusuudistus/uusi_tietojarjestelma)

Näillä näkymin ERICA palveluja on harvoin tarve käyttää kentältä, langattoman laajakaistayhteyden läpi. ERICA käyttö keskittyy lähinnä pelastuslaitosten tilannekeskuksiin ja toimistokäyttöön.

KEJO

KEJO hanke oli jo käynnissä VOTI ja TUPO hankkeiden käynnistyessä. KEJO hankkeessa määritellään ja toteutetaan turvallisuusviranomaisten yhteinen kenttä(johtamis)järjestelmä. Pelastustoimessa käytössä oleva PEKE (Pelastustoimen kenttäjohtamisjärjestelmä) tullee korvautumaan KEJOlla aikanaan.

KEJO ja sen saaminen pelastustoimen käyttöön voidaan nähdä hyvin tärkeänä, jollei tärkeimpänä pelastustoimen IT hankkeena tällä hetkellä. Tästä johtuen hankkeessa KEJOn käyttöön liittyvät verkkotekniset ja etenkin tietoturva-asiat ovat nousseet keskiöön. TUPO hankkeen tutkija onkin toiminut tietoturvan asiantuntijana KEJOn tietoturvatyöpajoissa. Jo MoniKa hankkeen aikana koetettiin viestittää KEJO hankkeen päättävälle taholle, ettei koko järjestelmää "leimattaisi" tietylle suojaustasolle, vaan järjestelmä mahdollistaisi useamman suojaustason tiedon säilyttämisen ja käytön. Näin kuntasektorin käyttäjät voisivat käyttää järjestelmää esimerkiksi ST4 ympäristöistä ja järjestelmästä saatavan tiedon suojaustasoluokitus määräytyisi käyttäjän ja hänen käyttöympäristönsä mukaan. Näin matalamman suojaustason omaava käyttäjä/ympäristö saisi käyttöönsä vain suojaustason mukaista tietoa.

TUVE

TUVE (Valtion Turvallisuusverkkohanke) tuottaa korkean turvallisuustason tietoverkon jota tulee operoimaan Suomen Turvallisuusverkko OY (Erillisverkot Oy:n tytäryhtiö). Valtiovarainministeriön sivuilta löytyy yleiskuvaus hankkeesta:

Hallinnon turvallisuusverkkohankkeessa (TUVE) suunnitellaan ja toteutetaan valtion ylimmälle johdolle ja yli 30 000 turvallisuusviranomaiskäyttäjälle oma korkean varautumisen tietoverkko tarvittavine palveluineen. Verkon käyttäjiksi tulevat valtion ylimmän johdon ja ministeriöiden lisäksi valtion yleisen järjestyksen ja turvallisuuden, pelastustoiminnan, meripelastustoiminnan, rajaturvallisuuden, hätäkeskustoiminnan, maahanmuuton, ensihoitopalvelun sekä maanpuolustuksen kannalta keskeiset viranomaiset.
(http://www.vm.fi/vm/fi/05_hankkeet/024_tuve/index.jsp)

TUVE verkkoa varten on valmisteltu omaa lakiaan, ja hallituksen esitys laista on löydettävissä mm. eduskunnan sivuilta *"Hallituksen esitys eduskunnalle laeiksi julkisen hallinnon turvallisuusverkkotoiminnasta ja viestintämarkkinalain 2 §:n muuttamisesta"*.
(http://217.71.145.20/TRIPviewer/show.asp?tunniste=HE+54/2013&base=erhe&palvelin=www.eduskunta.fi&f=WORD)

Mitä ilmeisimmin ERICAn ja KEJOn tuotantoympäristöt tulevat sijaitsemaan TUVEn sisällä ja liikennöinti näihin palveluihin on mahdollista vain TUVEn kautta. Tämä on pyritty huomioimaan TUPO hankkeessa alusta lähtien. VOTIn osalta hankkeen kestäessä alkanut KUNTU hanke muutti VOTIn fokusta siten että TUVE palvelujen saatavuuden problematiikka kuntasektorin näkökulmasta jätettiin tarkastelun ulkopuolelle.

KUNTU

KUNTU hankkeen tehtävänä on selvittää ja toteuttaa kuntaviranomaisten liittyminen TUVE verkkoon. Niin VOTI kuin TUPO hankekaan ei ollut mielestämme riittävästi yhteistyössä KUNTU hankkeen kanssa. KUNTUsta on verraten vähän julkista tietoa saatavilla, joten hanketta ei voida tässä raportissakaan käsitellä kovin laajasti.

VARANTO

VARANTO hankkeen tavoitteena on tuottaa pelastustoimen yhteinen tietovaranto. Koska pelastustoimen tietoturvaan liittyvillä asioilla on vahva merkitys VARANTO hankkeessa, osallistu TUPO hankkeen tutkija tietoturvaselvityksen tekemiseen, jossa käytiin läpi VARANTO hankkeen tietoturvamäärittelyihin vaikuttavaa lainsäädäntöä, yleisiä ohjeistuksia sekä itse VARANTO järjestelmän riskianalyysiä. Tulos ilmestyi pelastusopiston julkaisusarjassa nimellä VARANTO ja tietoturva.

Tehty selvitystyö edelleen vahvisti sitä käsitystä, että pelastustoimen varsin heterogeeninen käyttäjäkunta tarvitsee tietojärjestelmältä skaalautuvaa suojaustasomäärittelyä. Tällä tarkoitetaan sitä, että samassa tietojärjestelmässä voi olla julkista tietoa ja salassa pidettävää tietoa eri suojaustasoilla. Käyttäjän oikeudet, päätelaitteen suojaustaso sekä tarve tietoon määrittelevät, mitä tietoa käyttäjä voi järjestelmästä saada.

VARANTO tietomallin pohjalta alettiin määritellä suojaustasoja lähtökohtana atomaarinen suojaustasojen määrittely. Tällä tarkoitettiin sitä että jokainen yksittäinen tieto saisi oman suojaustasomäärityksensä. Loppujen lopuksi todettiin tämä lähestymistapa mahdottomaksi toteuttaa ja samalla havaittiin, että oikea

tapa rakentaa tällainen suojaustasojärjestelmä on näkymäkohtainen suojaustasoluokittelu. Näkymäkohtaisessa suojaustasoluokittelussa suojaustaso määräytyy kunkin käyttäjälle tarjottavan näkymän osalta ja yhdessä näkymässä voi myös olla eri suojaustasolla olevia alinäkymiä. Tätä mallia myös ehdotettiin KUNTU hankkeen edustajalle hankkeen esittelytilaisuudessa.

VOTI hanke

VOTI hanke alkoi 1.9.2014 ja päättyi 31.8.2014. Hankkeen rahoitus tuli pääosin Palosuojelurahastolta. Hankkeen toteuttamisesta vastasi Pelastusopiston tutkimusyksikkö. Hankkeessa toimi yksi työntekijä päätoimisesti, toinen osa-aikaisesti.

Ulkoiset vaatimukset

Hankkeen yhtenä vahvana alkuunpanija on ollut tieto pelastustoimen mahdollisesta liittymisestä tulevaan TUVE-verkkoon, kuten myös uusien tietojärjestelmien kuten KEJO ja ERICA käyttöönotto lähivuosina.

Yhdeksi tärkeäksi ulkoiseksi vaatimukseksi muodostui siis näiden uusien järjestelmien asettamat tietoturva- ja mahdolliset laitteistovaatimukset

Toinen tärkeä tunnistettu ulkoinen tekijä oli pelastuslaitoksen ICT-ympäristön ja palveluiden tuottaja, eli toistaiseksi käytännössä kunta ja heidän vaatimuksensa. Tältä osin vaatimukset kohdistuivat lähinnä tietoturvaan ja pääsyyn kunnan palveluihin ulkoisesta verkosta käsin. Laitteiston osalta pelastuslaitosten operatiivisen toiminnan tarpeet poikkeavat huomattavasti kunnan muusta laitekannasta ja tältä osin mitään selkeää vakiointia ei tämän suhteen oikeastaan ole ollut olemassa paria poikkeusta lukuun ottamatta.

Selvitystyö

Hankkeen aikana pyrittiin tutustumaan mahdollisimman laaja-alaisesti pelastustoimen operatiivisen toiminnan nykyiseen laitekantaan, järjestelmiin ja toimintatapoihin eri puolilla Suomea. Valitettavasti aika eikä kustannukset sallineet kaikilla pelastuslaitoksilla vierailua, mutta uskoimme saaneemme kohtuullisen hyvän kuvan kokonaisuudesta nykyiselläkin otannalla.

Selvitysten aikana kävi nopeasti selväksi, että oikeastaan jokaisella laitoksella on omia toimintamallejaan, laitekanta on hyvin kirjava ja olemassa olevan tietoturvan taso on liki olematon. Useimmiten ICT-palvelut tulevat kunnilta tai yritykseltä joka tuottaa ko. palvelut kunnalle. Laitoksilla on jossain määrin myös omaa osaamista ja tietotaitoa ICT-asioissa, käytännössä arkirutiinien pyörittäminen tuntuu vain syövän suurimman osan ajasta jolloin kehityshankkeille ei juurikaan jää aikaa eikä voimia.

Tietoliikenteessä käytetään yleisimmin kuntien verkkoa, josta käytettävät peruspalvelut kuten sähköposti tai videoneuvottelu saadaan erilaisilla kaupallisilla 3/4g tai @450 yhteyksillä yksittäisille työasemille käytettäväksi kentälle operatiivisen toiminnan tukena.

Tärkeäksi koetut palvelut

Tehtyjen selvitysten perusteella laadittiin lista palveluista joita vakioidusta työasemasta täytyy pystyä käyttämään ja jota vakioinnin tulee omalta osaltaan tukea.

1. Tilannekuva, kenttäjohtaminen (PEKE, MERLOT, KEJO)
2. Kohdetietopalvelu (rakennukset, ajoneuvot, turvalaitteet)
3. Taustatietopalvelu (Luova, Tokeva, Boris, Usva, yms)
4. Kunnalliset palvelut (email, verkkolevy, kartat, intra) helposti käytettävissä
5. Tilannepäiväkirja (helppokäyttöinen usean toimijan bloki: auto / tike / joke)
6. Tiedonsiirtopalvelut (offline kansiot, smartboard, eBeam, videoneuvottelu)

7. Toiminnanjaotus
8. Videokuva (ajoneuvosta, kohteesta, toiselta viranomaiselta, lämpökamera, yms)
9. Anturidata (sää, ajoneuvon vesi ja vaahto, pelastajan elintoiminnot, yms.)
10. Liikennevalojen ohjaus (nykyään useita toteutuksia)

Käyttöympäristö

Hankkeen alkaessa oli hyvin epäselvää mitä KEJO ja ERICA tulevat vaatimaan käyttöympäristöltään ja kuinka tietoliikenneyhteydet niihin tullaan järjestämään. KEJO:n käytön osalta puhuttiin pitkään ST III tason vaatimuksista, joiden saavuttaminen pelastustoimessa vaikutti jo selvitystyömme perusteella kohtuullisen haastavalta ja ennen kaikkea erittäin turhalta kustannustekijältä.

Vakioinnin näkökulmasta asiasta voisi tiivistäen sanoa, että ST III tason tuominen pelastustoimen työasemiin muuttaa kustannukset moninkertaiseksi ja tekee useiden käytännön asioiden toteuttamisen hankalaksi, erittäin kalliiksi, jollei jopa mahdottomaksi tuomatta kuitenkaan mitään selkeää etua pelastustoimelle.

Tältä pohjalta olemme esittäneet lukuisissa yhteyksissä pelastustoimen ICT-ympäristön pitämistä ST IV tasolla PEIP-verkossa, ajatuksen kuitenkaan saamatta juurikaan vastakaikua.

Hankesuunnitelma

Selvitystyön tulosten perusteella laadittiin hankkeelle sisäinen suunnitelma, jossa tavoitteeksi otettiin tuottaa ensimmäisen vuoden aikana ST IV tason tietoturvan vaatimukset täyttävä, mutta kohtuullisen hintainen vakioitu työasema ja pilotoida sitä todellisessa ympäristössä ja mahdollistaa tärkeimpien yllä listattujen palveluiden käyttäminen siinä.

Saman aikaisesti päätettiin myös lähteä rakentamaan tämän jälkeen toteutettavien palveluiden kehittämiseksi tarvittavaa infraa, eli pystyttämään oma kehityspalvelin PEIP-verkkoon, luomaan yhteyksiä sinne sekä hankkimaan tarvittavia antureita, kameroita yms. sekä testaamaan näitä.

Suunnitelman toista vaihetta varten on tarkoitus hakea jatkohanketta ja kehittää sekä toteuttaa listan loppupuolen palveluita ja tuoda niitä pelastustoimen yhteisesti käytettäväksi.

Tulevaisuuden visio

Koko hankkeen visiona oli tulevaisuuden toimintamalli, jossa ajoneuvossa on keskitetty laite joka:

- toimii täysin itsenäisesti ja automaattisesti
- mahdollistaa kaikkien tarvittavien lisälaitteiden liittämisen
- hoitaen autosta kerättävän tiedon ja anturidatan käsittelyn ja puskuroinnin
- välittämisen eteenpäin keskitettyihin tietojärjestelmiin
- näyttämisestä reaaliajassa TIKE, JOKE

Kaikki tieto mitä kentältä kerätään (sää, paikka, ääni, kuva, pelastajan elintoiminnot, yms.):

- on käytettävissä ajoneuvossa
- kaikkialla peip verkossa reaaliajassa (TIKE, JOKE).
- kaikki tieto myös tallennetaan automaattisesti

- jakamaan helposti halutuille ihmisille myös oman laitoksen ulkopuolelle
- tarkastelemaan jälkeenpäin vaikkapa aikaperspektiivissä.

Kiinteän ajoneuvotyöaseman pilotointi

Tavoitteena oli pilotoida tuotettu vakiointi oikeassa toimintaympäristössä, joten lähdimme rakentamaan soveltuvaa laitteistoa ja ympäristöä tätä varten heti hankkeen alussa.

Ympäristöä rakennettaessa pyrittiin huomiomaan esiin nousseita vaatimuksia ja tarpeita mahdollisimman monelta kannalta ja luomaan ympäristö joka vastaisi myös käyttäjien toiveita niin käytettävyydeltään kuin vaikkapa ergonomialtaan. Ympäristöstä haluttiin mahdollisimman "konttorimainen" (kuva 1), isot näytöt ja kunnollinen näppäimistö ja hiiri.

Kuva 1 Työaseman näyttöjen ja oheislaitteiden sijoittelu

Pilottiympäristöksi valikoitui Pohjois-Savon pelastuslaitoksen johtoauto, PRS32, kuvassa2. Syynä johtoauton valintaan oli lähinnä siinä tarvittavat ja käytettävät laajemmat palvelut. Mikäli kaikki johtoautossa tarvittava saadaan toimimaan, saadaan sammutusautossa tarvittavat asiat toteutettua tästä karsimalla.

Kuva 2 VOTI hankkeen pilottiajoneuvo

Laitteistoksi valittiin Sunit Oy:n kiinteä ajoneuvotietokone mallia FD2 (kuva 3). Yhtenä valintakriteerinä oli poliisin juuri tekemä hankinta vastaavasta laitteesta, jolloin uskoimme mahdollisten KEJO tuomien vaatimusten ainakin täyttyvän laitteiston osalta.

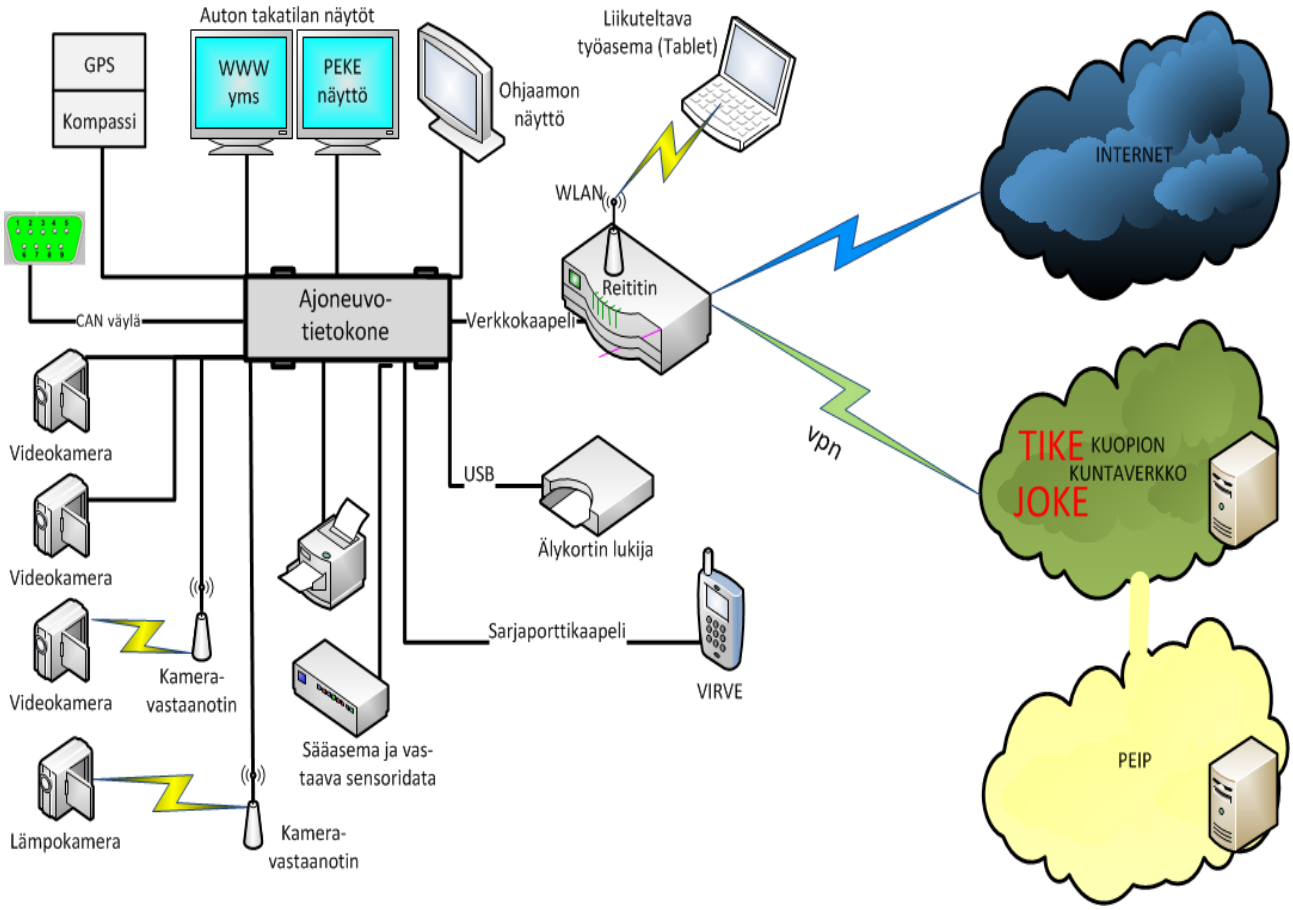
Kuva 3 Pilotissa käytetty työasemalaitteisto

Sunit:in laitteet ovat yleisesti ottaen ajoneuvotietokoneiden kentällä laadukkaina pidettyjä joskin myös hieman kilpailijoitaan kalliimpia. Vierailumme Sunit Oy:n tuotantotiloissa ja tutustuminen heidän tuotanto- ja testauskäytäntöihinsä antoivat kuitenkin erittäin hyvän kuvan tuotteiden laatuun panostamisesta ja sitä kautta perusteita ehkä hieman korkeammalle hinnalle.

Ajoneuvoon asennettiin

- Sunitin uusin ajoneuvotietokone
- 2 kpl 20" näyttöjä takatilaan + 7" karttanäyttö kuljettajalle
- Axis videoserveri + valvomo-ohjelmisto
- Bullard langaton lämpökamera
- Goodmill monikanavareititin
- kiinteä dataradio VIRVE-data:a varten

Kaaviona asennusjärjestely on esitetty kuvassa 4.



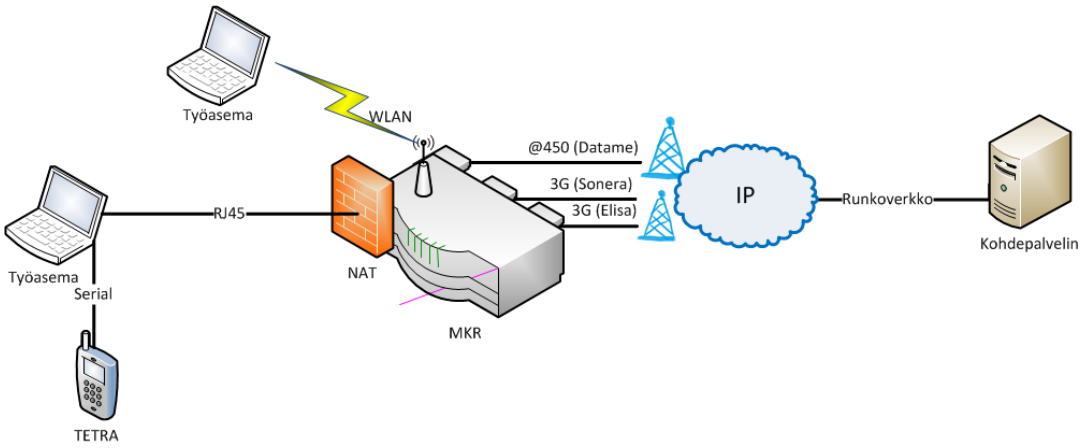
Kuva 4 VOTI pilottiympäristön komponentit ja niiden väliset yhteydet

Kokonaisuudessa pyrittiin alusta alkaen "palomies" ystävälliseen toimintaan, eli kaiken pitäisi olla käytettävissä helposti ja yksinkertaisesti. Ohjelmistojen osalta lähdettiin aivan perusasioista liikkeelle ja pyrittiin saamaan niiden toiminnallisuus kuntoon, eli PEKE:n karttanäytön saamiseen kuljettajalle sekä sähköpostiin ja pääsyyn verkkolevyille.

Pääsyn kunnan palveluihin toteutti Kuopion ICT-palveluista vastaava Istekki Oy. Pääsy toteutettiin F5 portaali ratkaisulla, käyttäjien kirjautuessa omalla tunnuksellaan normaalia selainta käyttäen kunnan portaalin, jossa jokaiselle on näkyvissä hänelle määritellyt tarjolla olevat palvelut. Käytettävät ohjelmat voivat olla portaalin sisällä tai ne voidaan tuoda ajoneuvon tietokoneelle terminal-server tyylisesti

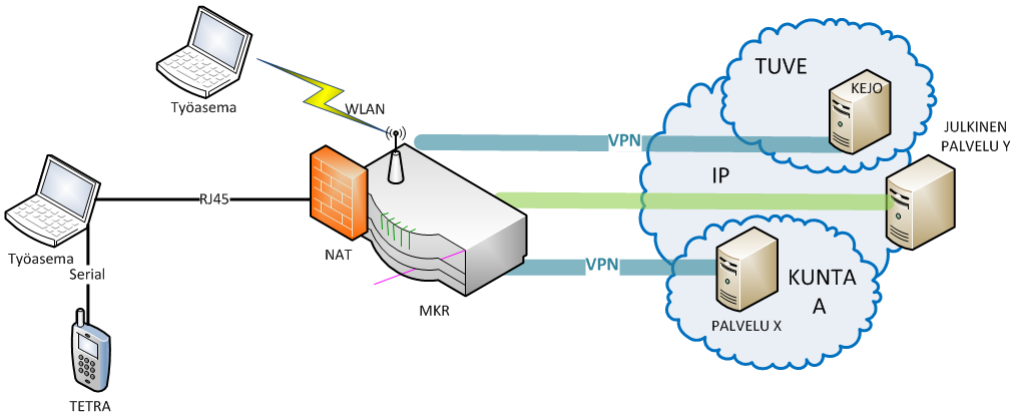
julkaistuina sovelluksina, jolloin esim. Outlook aukeaa ajoneuvon koneelle omaan ikkunaansa aivan kuin se olisi koneessa paikallisesti oleva sovellus.

Tietoliikenneyhteydet ajoneuvoon oli rakennettu jo aiemmin MoniKa -hankkeen yhteydessä. Ajoneuvoon oli asennettu tällöin Goodmil W24R monikanavareititin, jossa oli kaksi 3G yhteyttä ja @450 yhteys. Datame Oy:n mentyä konkurssiin, @450 yhteys jäi käyttämättömäksi, joten yhteys oli käytännössä kahden eri operaattorin 3G yhteyksien varassa. Lisäksi itse ajoneuvotietokoneessa oli VIRVE yhteys. Yhteyksien rakentumista on kuvattu alla olevassa kuvassa 5.



Kuva 5 Tietoliikenteen rakentuminen VOTI pilotissa

Varsinaisten tietoliikenneyhteyksien varaan rakennettiin loogisia yhteyksiä (kuva 6), kuten yllä kuvattu portaaliratkaisu. Tavoitteena oli saada yhteys PEIP verkkoon VPN ratkaisulla, mutta tämä jäi hankkeen päätyessä vielä kesken. KEJO palvelun pääsyn hallinnan ja tietoverkkoratkaisun tarvitsemat osat oli hankkeen alussa ajatus tuottaa PEIP -yhteyden avulla, mutta hankkeen aikana todettiin että nämä asiat määrittelee KUNTU hanke.



Kuva 6 Loogiset tietoliikenneyhteydet pilotin kannalta

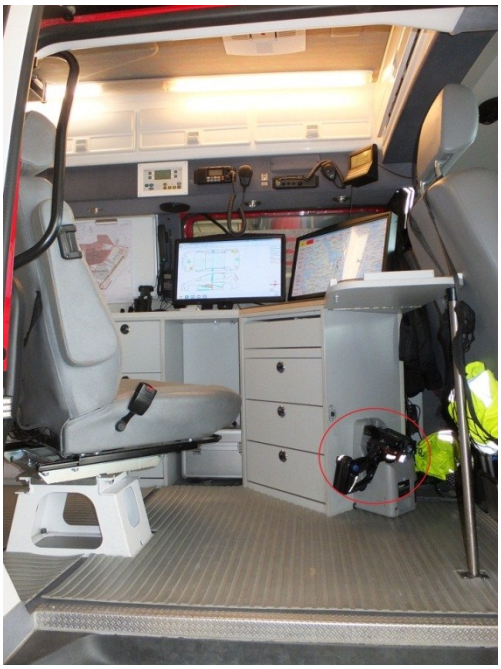
Pilotin kokemukset ja palaute

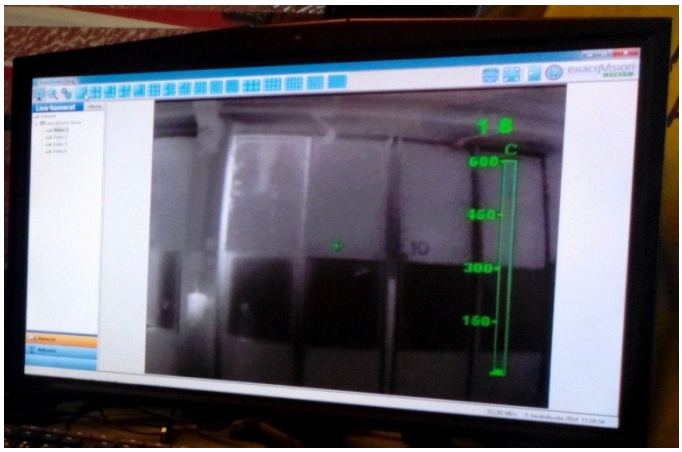
Laitteiston esitestauksen aikana hieman ylimääräistä työtä aiheutti koko koneen täydellinen jumiutuminen PEKE:n asennuksen jälkeen. Ongelma saatiin paikallistettua Sunitin uuden koneen sarjaportin ajureiden ja PEKE:n gps:n rajapinnan väliseksi ja korjauskin siihen saatiin varsin nopeasti saman ongelman vaivatessa myös poliisia heidän tehdessä omia testejään samanlaisilla työasemilla.

Laitteisto on ollut kesän toukokuusta 2014 alkaen operatiivisessa käytössä ja palaute käyttäjiltä on ollut hyvää pienten alkuvaikeuksien jälkeen. Ergonomiaa ja työympäristöä on kehuttu. Hyvin toimivat ja helposti ajonaikanakin käytettävät yhteydet kunnan palveluihin ja mm. Pronto:on on koettu hyödylliseksi. Kokonaisuus, jossa P3 voi operoida kahdella isolla näytöllä ja kuljettajalle on PEKE:n reititys omalla näytöllään (kuva 7) auki on koettu erityisen toimivaksi.

Kuva 7 Näyttöjen sijoittuminen ajoneuvoon

Langattomasta lämpökamerasta ei ole koettu olevan ainakaan tällaisellaan suurta hyötyä, mikäli laitteita olisi kentällä enemmän ja niiden kuva saataisiin aina tarpeen mukaan johtoautoon tai TIKE:en voisi tilanne olla erilainen. Käyttö sinällään koettiin helpoksi, laite katkaisijasta päälle ja valvomo-ohjelmisto käyntiin tietokoneella jonka jälkeen kuva on nähtävissä (kuva 8).





Kuva 8 Lämpökameran sijoittelu (vasemmalla) ja lämpökamerakuva ajoneuvon näytöllä (oikealla)

Koko laitteiston yhteinen virrankulutus on kohtuullisen suuri ja laitteiden ollessa aina päällä tämä on aiheuttanut pientä huolta tilanteissa jossa autolla ollaan pidempään paikallaan ilman ulkoista sähkönsyöttöä.

TABLET-tietokoneet

Kannettavien laitteiden kehitys aivan viimevuosina on ollut nopeaa, erityisesti TABLET-tyyliset laitteet ovat yleistyneet huimaa vauhtia ja kiinnostus niiden käyttöön pelastustoimessakin oli selvästi havaittavissa.

Normaalien kannettavien tietokoneiden ja kiinteiden ajoneuvotyöasemien lisäksi tavoitteena oli, että vakiointi mahdollistaa myös TABLET-laitteiden käytön. Testausta varten hankittiin Aava Mobilen Inari 3G tablet (kuva 9). Laite on varustettu Windows 8.1 käyttöjärjestelmällä ja siinä on sisäinen 3G yhteys sekä GPS. Laite ei ollut hankintavaiheessa vielä kaupallisessa myynnissä, vaan kyseessä on kehityssarjan tuote joten emme tässä suoranaisesti arvioi tai testaa itse laitetta sen tarkemmin.

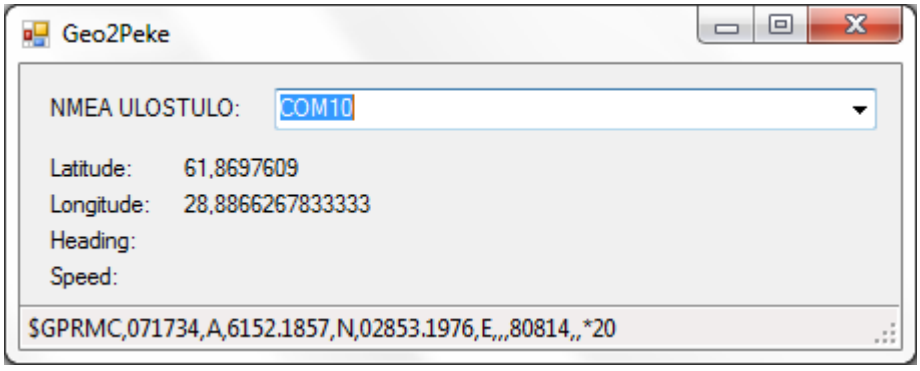
Kuva 9 Testikäytössä oleva Aava Mobilen Inari 3G tablet

Laitteessa on IP65 luokittelu ja parin kuukauden satunnaisen käytön perusteella se on mekaanisesti ihan kohtuullisen asiallinen. Ehkä joku kuminen suojakuori laitteen reunojen ympärillä tekisi siitä vielä sopivamman pelastuslaitosten käyttöön. Laitteen mukana tuli telakka, jota voi kyllä käyttää ajoneuvossakin, mutta se on selvästi suunniteltu enemmän pöydällä pidettäväksi. Akun kesto tuntuu olevan ihan hyvä, useita tunteja GPS päällä ja 3G yhteys auki PEKE:ä satunnaisesti käyttäen.

Laitteeseen asennettiin PEKE, itse asennus sujui ongelmitta (kuva 10). Suurimman ongelman PEKE käytölle aiheuttaa Windows 8.1:n mukanaan tuoma muutos jossa GPS:n tietoa ei enää saa ulos sarjaportista vaan Windowsin sijaintitietoa tarjoavasta järjestelmäpalvelusta. Tämä käytännössä rikkoo kaikkien perinteisestä sarjaportista GPS-tietoa lukevien ohjelmien yhteensopivuuden laitteen kanssa.

Kuva 10 PEKE Aava Mobile tabletissa

Jotta laitetta ja sen paikannusominaisuuksia saatiin ylipäätänsä testattua, tehtiin hankkeen ulkopuolella apuohjelma (kuva 11) joka generoi Windowsin sisäisestä sijaintitiedosta NMEA muotoista dataa ja lähettää sen virtuaalisen sarjaporttiin jonka PEKE voi avata kuten ennenkin. Tällä ratkaisulla PEKE:n paikannuskin saatiin toimimaan.



Kuva 11 PEKE käytössä tarvittu apuohjelma

Paikannustarkkuus ja herkkyys tuntuvat olevan tällaisten laitteiden normaalia GPS tasoa, eli ihan hyvä ja riittävä silloin kun kaikki toimii ja yleensä kun laite löytää paikkansa, toimii se sen jälkeen varsin luotettavasti tuntikausiakin.

Käyttäjän kannalta ongelmalliseksi tämän uuden Windowsin sijaintipalvelun tekee se, että poiketen perinteisestä sarjaportista jonka kerran aukaistuasi tiesi varmuudella olevan auki, tässä nykyisessä mallissa ei ainakaan kirjoittajan tietämyksen mukaan voi selkeästi pakottaa GPS:ää aina päälle. Testauksen aikana kävi joitakin kertoja niin, että sijainti katosi tilanteissa joissa ei varmuudella voinut olla kyse GPS signaalin heikkoudesta johtuva ongelma. Ongelman esiintyminen tuntui olevan jotenkin sidoksissa WLAN yhteyksien / 3G yhteyksien vaihtumisiin.

Toinen selkeä ongelma tulee siitä, että useat GPS paikkaa käyttävät ohjelma pyrkivät asettamaan järjestelmän kellonajan GPS:n mukaiseksi. Mikäli NMEA tieto generoidaan yllämainitulla tavalla, joudutaan siihen ottamaan aikaleima käyttöjärjestelmästä. Tämä aiheuttaa siis loputtoman kierteen, jossa aika otetaan ja säädetään saman lähteen perusteella.

Videokuvan välitys

Yksittäisenä esiin nousseena toiveena kentältä päin oli videokuvan siirto ajoneuvosta tilannekeskukseen. Lähes kaikilla laitoksilla asia oli vähintäänkin selvityksessä, joillakin laitoksilla asia oli jo toteutettu itsenäisesti koska tarjolla ei ole yhtenäistä ja yhteistä ratkaisua. Mikäli asiaan ei saada yhtenäistä määrittelyä aikaiseksi, muodostuu jälleen 22 erilaista järjestelmää jotka eivät ole keskenään yhteensopivia.

Asian tiimoilta päätettiin perustettiin kesällä 2014 "työryhmä" jonka tavoitteena oli testata ja määritellä yhtenäinen järjestelmä videokuvan siirtoa varten pelastustoimeen. Osallisina oli pelastusopiston T&K-yksikön lisäksi edustajat neljältä pelastuslaitokselta: Juha Alahäivälä (Jokilaaksojen pelastuslaitos), Mika Keränen (Pohjois-Karjalan pelastuslaitos), Heikki Kervinen (Länsi-Uudenmaan pelastuslaitos) sekä Tero Haapala (Kanta-Hämeen pelastuslaitos)

VOTI hankkeen puitteissa olimme jo hieman testanneet eri järjestelmiä ja laitteistoja. Järjestelmän pilottia varten hankittiin AXIS Q7404 videomuunnin (kuva 12) johon kytkettiin lämpökamera ja hankkeen jatkon aikana tarkoitus oli kytkeä muitakin kameroita sekä testata näiden toimintaa ja kuvan välittämistä TIKE:en.

Kuva 12 Pilotissa käytetty AXIS videoserveri

Tältä pohjalta sekä yleisen tulevaisuuden visiomme mukaisesti määrittelimme haluttuja ominaisuuksia järjestelmällä:

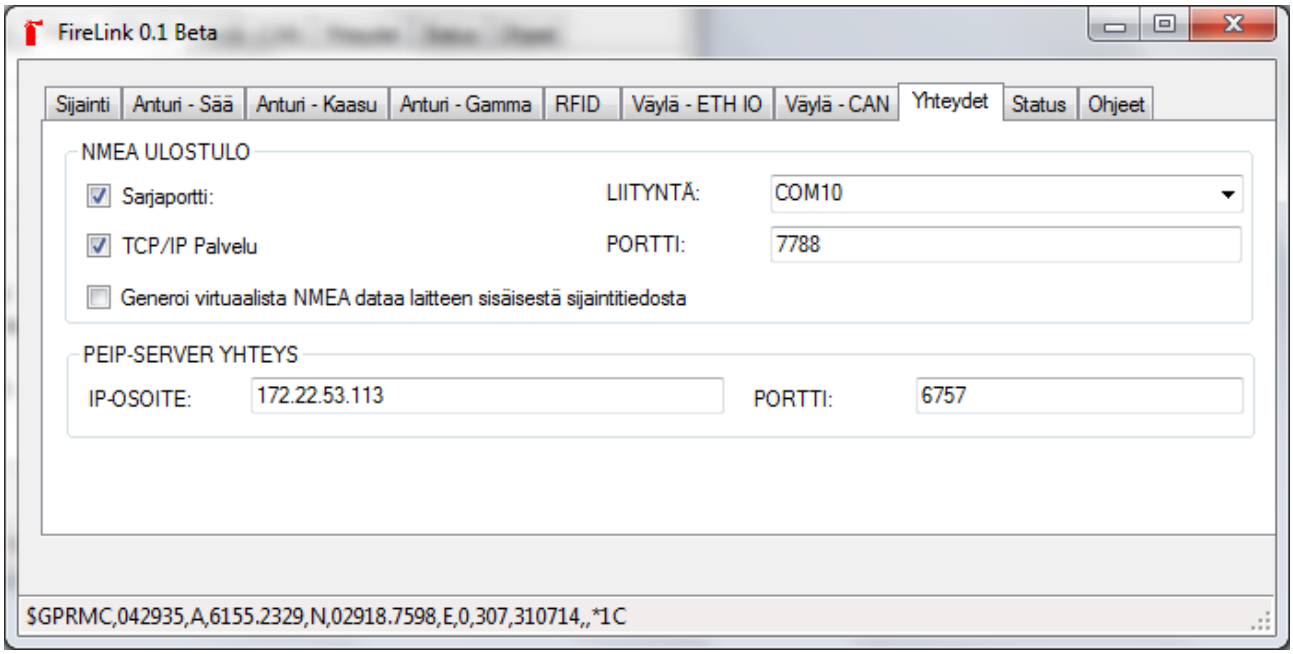
- laiteriippumaton -> voi käyttää eri valmistajien kameroita
- täysin skaalautuva -> yhden laitoksen yhdestä kamerasta koko suomeen ja ~1000 kameraan, hankittavissa vapaasti laitosten oman tarpeen mukaan
- tallennus -> kattavat tallennus, haku, arkistointi ja automaattisen poiston ominaisuudet
- hajautettu tallennus -> mahdollisuus määritellä fyysinen tallennuspaikka vapaasti
- tuki fiksulle offline tallennukselle -> ajoneuvon ollessa verkon ulkopuolella tai huonolla mkr-yhdeydellä maaseudulla puskuroituu kuva autoon, automaattinen siirto palvelimelle auton tultua esim. aseman wlan verkkoon
- kameroiden etäohjaus -> dome yms. käänneltävien kameroiden ohjattavuus ilman lisälaitteita
- tuki ulkoisen kuvan tuontiin järjestelmään -> hätäkeskus, videopuhelu, ip-stream soittajan kännykästä tapahtumapaikalta, videoneuvottelulaitteisto
- mahdollisuus kuvan katseluun mobiililaitteilla. Mielellään tarvittaessa julkisen verkon kauttakin
- kattava käyttäjien hallinta -> yhteinen koko suomeen, kuitenkin myös niin että laitokset voivat vapaasti hallinnoida itse omiaan. Pitää pystyä nopeasti ja helposti myöntämään oikeus kenelle tahansa mihin kameraan/näkymään tahansa

Tiedon keruu ja anturit

Vakioitu työasema tarjoaa myös hyvän alustan toteuttaa yhtenäinen anturitiedon keruu, siirto ja jakamisväylä koko pelastustoimelle. Hankeen merkittävänä osana oli alusta alkaen lähteä rakentamaan järjestelmää siten, että itse työaseman perusvakioinnin päälle saadaan seuraavassa vaiheessa luotua toimiva konsepti jossa kaikki ajoneuvon ympäristössä olevat mittarit ja anturit saadaan liitettyä ajoneuvoon ja näiden tieto välitettyä eteenpäin haluttuun kohteeseen PEIP-verkkoa myöten.

Tiedon siirron ja liityntöjen tekeminen erilaisiin laitteisiin ei kuulunut vielä tämän hankkeen sisältöön, mutta laitteiden järkevän testaamisen helpottamiseksi ja seuraavassa vaiheessa suunniteltujen asioiden edistämiseksi hankkeen ulkopuolella tehtiin useita apuvälineitä ja ohjelmistoja puhtaasti työntekijöiden henkilökohtaisen mielenkiinnon vuoksi.

Ajoneuvon puoleen rakennettiin liityntäohjelmisto (kuva 13), joka mahdollistaa kaikkien kuviteltavissa olevien erilaisten antureiden kytkemisen, tiedon jakamisen ajoneuvon sisällä sekä välittämisen eteenpäin ajoneuvon ympäristöön WLAN:n kautta sekä PEIP-verkon palvelimelle.

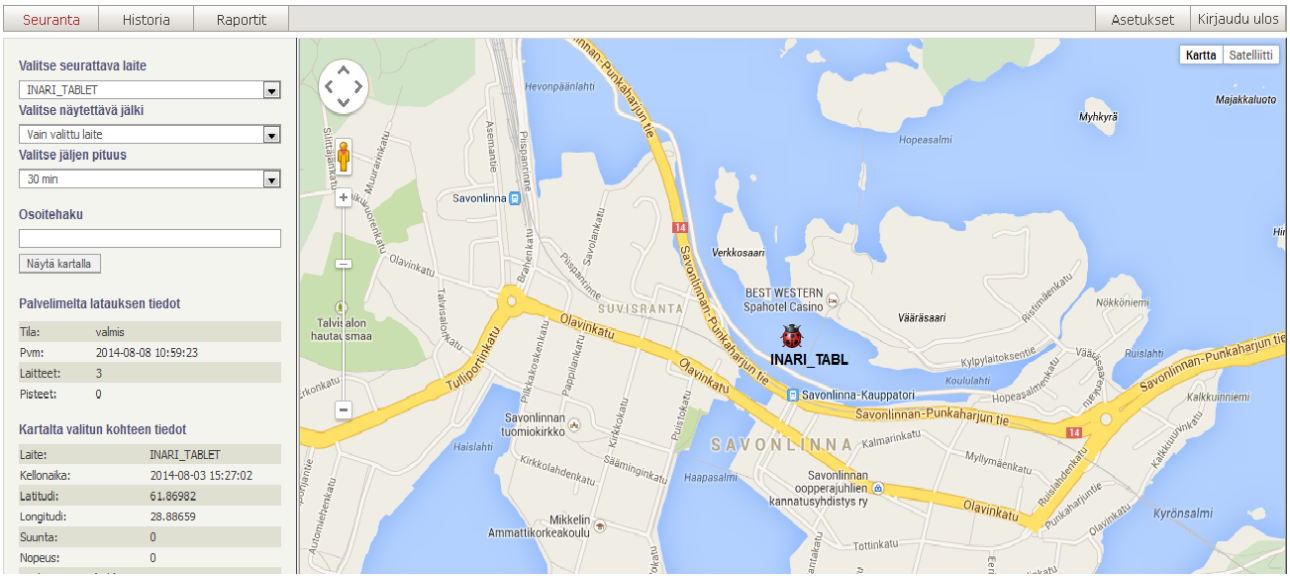


Kuva 13 Anturidatan liityntäohjelmisto

Järjestelmässä huomioitiin saman tiedon (esim. sijainti) jakamisen tarpeellisuus ajoneuvon sisällä useamman ohjelman kesken ja se mahdollistaa määriteltäväksi eri lähteistä luettavan datan yhdistämisen. Esim. sääaseman GPS-tietoa voidaan käyttää auton omana sijaintina, jakaa se eteenpäin PEKE:lle ja välittää tilannekeskukseen säätiedon mittauspaikkana, kun taas kaasuanturin sijaintitieto voi olla itse ajoneuvon sijainnista riippumaton, mittalaitehan voi olla useiden satojen metrien tai jopa kilometrien päässä ajoneuvosta.

Määriteltiin protokolla jonka mukaisesti tieto välitetään palvelimelle ja tehtiin tarvittavat ohjelmistot huolehtimaan tiedonsiirrosta molempiin päihin. Palvelimelle luotiin MYSQL pohjainen testitietokanta jonne ajoneuvosta mitattu data tallennetaan ja josta sitä voidaan jälkeenpäin tarkastella.

Tätä ja reaaliaikaista seurantaa varten luotiin yksinkertainen WEB-käyttöliittymä (kuva14), josta nähdään halutun kohteen sijainti kartalla sekä sieltä saatavissa olevat mittausarvot.



Kuva 14 web käyttöliittymä anturidatan tarkastelua varten

Ajoneuvon sääasema

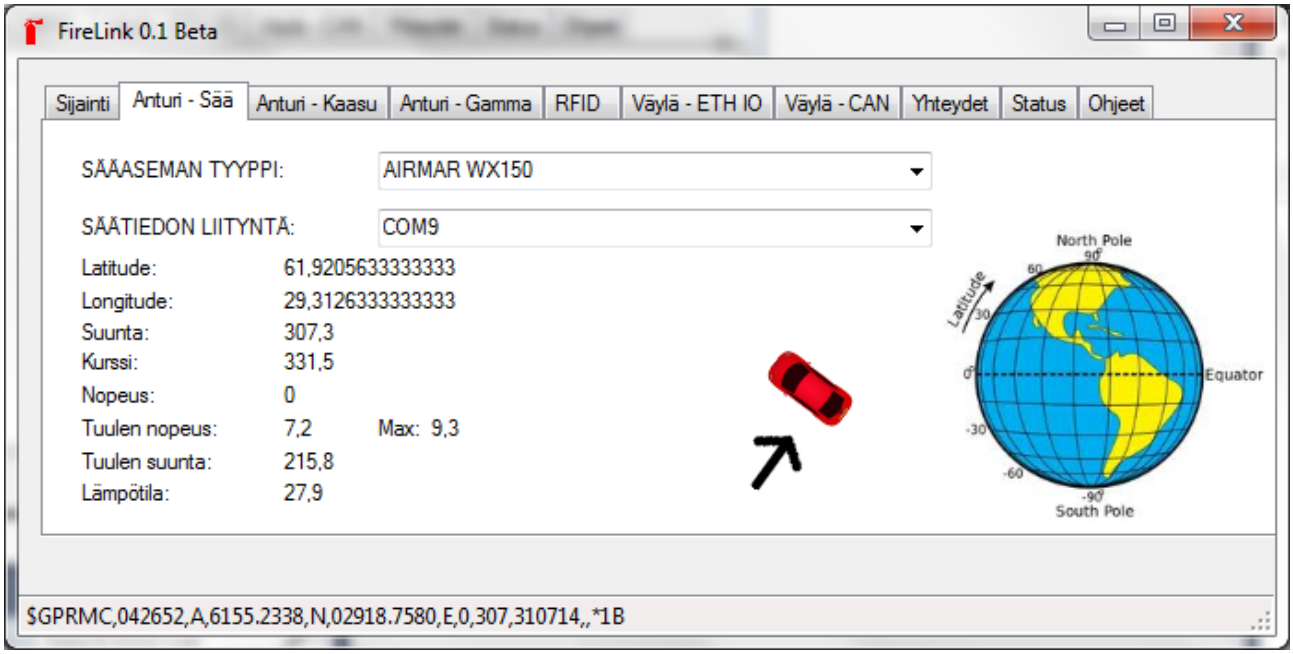
Testausta varten hankittiin ajoneuvoon sopiva sääasema mallia Airmar 150WX (kuva 15). Tämä on tarkoitettu ensisijaisesti merenkulkuun, mutta soveltuu erinomaisesti myös pelastustoimen käyttöön koska tuulen suunnan ja voimakkuuden mittaus perustuu ultraääneen eikä laitteessa ole mitään mekaanisesti liikkuvia osia. Laite voidaan siis asentaa ajoneuvoon kiinteästi, jolloin mittausdataa ajoneuvosta on saatavilla vaikkapa TIKE:en aina ilman käyttäjän erillisiä toimenpiteitä.

Kuva 15 Pilotissa käytetty sääasema

Laitteessa on sisäinen GPS jonka lisäksi siitä saadaan lämpötila, ilmanpaine, tuulen nopeus ja suunta sekä kallistuskulmat. Lisävarusteena laitteeseen voidaan hankkia sademäärä ja kosteus anturi sekä lämmitysvastus.

Laite osaa mitata tuulen nopeuden ja suunnan myös liikkuvasta ajoneuvosta ja parin kuukauden käytännön testauksen perusteella tämä toimii kohtuullisen hyvin. Laite on kuitenkin melko tarkka asennuspaikan suhteen, eli ajoneuvon aiheuttamat virtaukset vaikuttavat luonnollisesti mittaustulokseen. Samat ongelmat toki vaivaavat perinteisempiäkin antureita, joten yhteenvetona voisi todeta, että pelastustoimen tarpeisiin laite soveltuu varsin hyvin johtuen kiinteän asennuksen mahdollisuudesta.

Laitetta testattiin kesän ajan käyttäen testauksen helpottamiseksi luotuja apuohjelmia ja palvelimia (kuva 16).



Kuva 16 Säätieto sensoriohjelmistossa

Ajoneuvossa olevien antureiden mittaaminen

Itse ajoneuvosta on tarve mitata useaa erilaista tietoa, joista jokainen on saatavissa hieman erilaisen liitynnän kautta. Hankkeessa pyrittiin testaamaan edullinen ja yksinkertainen liityntälaite, jota voidaan käyttää hyvinkin erilaisissa tapauksissa halutun tiedon mittaamiseen.

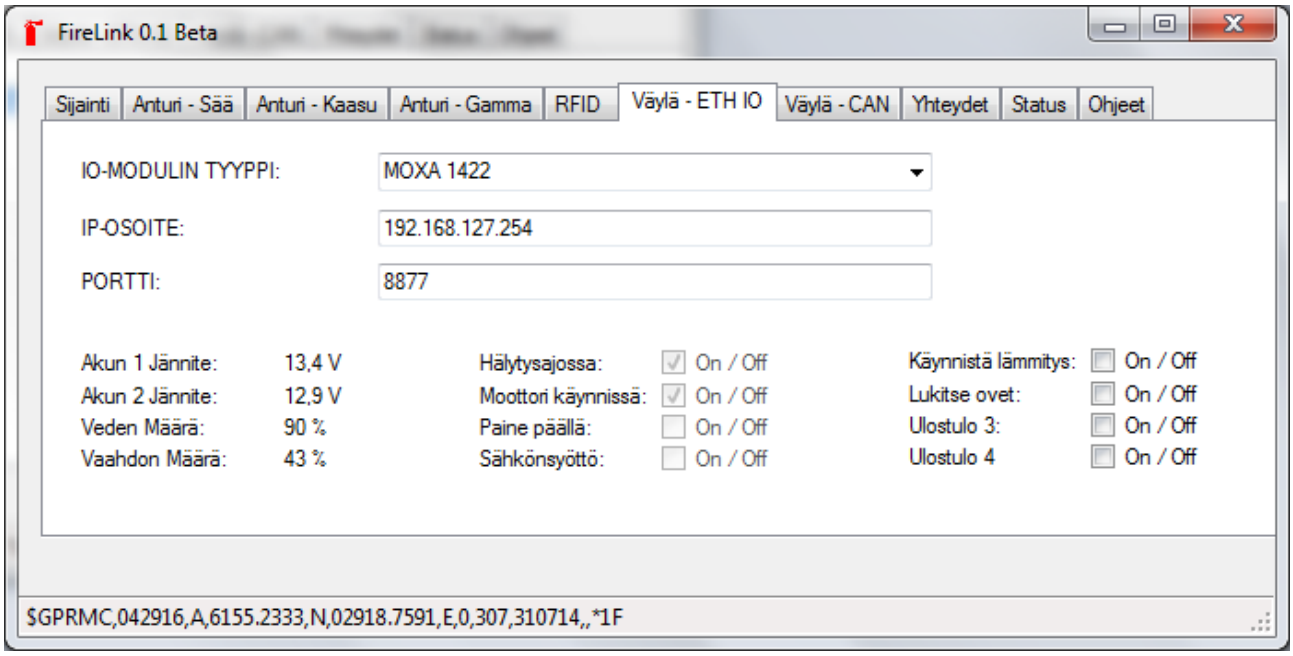
Liityntälaitteeksi valittiin MOXA E1424 ethernet IO moduli (kuva 17), joka mahdollistaa 4 analogista tuloa, 4 digitaalista tuloa ja 4 digitaalista lähtöä. Laite liitetään ajoneuvon sisäiseen ethernet verkkoon ja sitä kautta ajoneuvotietokoneeseen.

Kuva 17 Anturidatan liityntälaite

Anturiliitäntöihin voidaan tarpeen mukaan kytkeä halutut anturit ja välittää vaikkapa kohteeseen matkalla olevan ajoneuvon vesimäärästä tieto esim. TIKE:en tai prosessoida sitä automaattisesti palvelimella ja lähettää VIRVE kapulaan hälytys jos hallissa seisovan ajoneuvon akku on tyhjä.

Testauksen aikana laitteen analogiset mittakanavat kytkettiin käytettävissä olleen ajoneuvon akkuihin sekä tankkien antureihin ja digitaalisilla tuloilla seurattiin muutamien muiden yksittäisten laitteiden päällä oloa.

Laitteen mittaama tieto välitettiin reaaliajassa palvelimelle josta se oli internetin yli seurattavissa. Palvelimella testattiin myös automaattisen akkuhälytyksen lähettämistä SMS-viestinä akun jännitteen laskiessa alle määritellyn tason.



Kuva 18 Sensoritieto apuohjelmistossa

PEIP-verkon kehityspalvelin

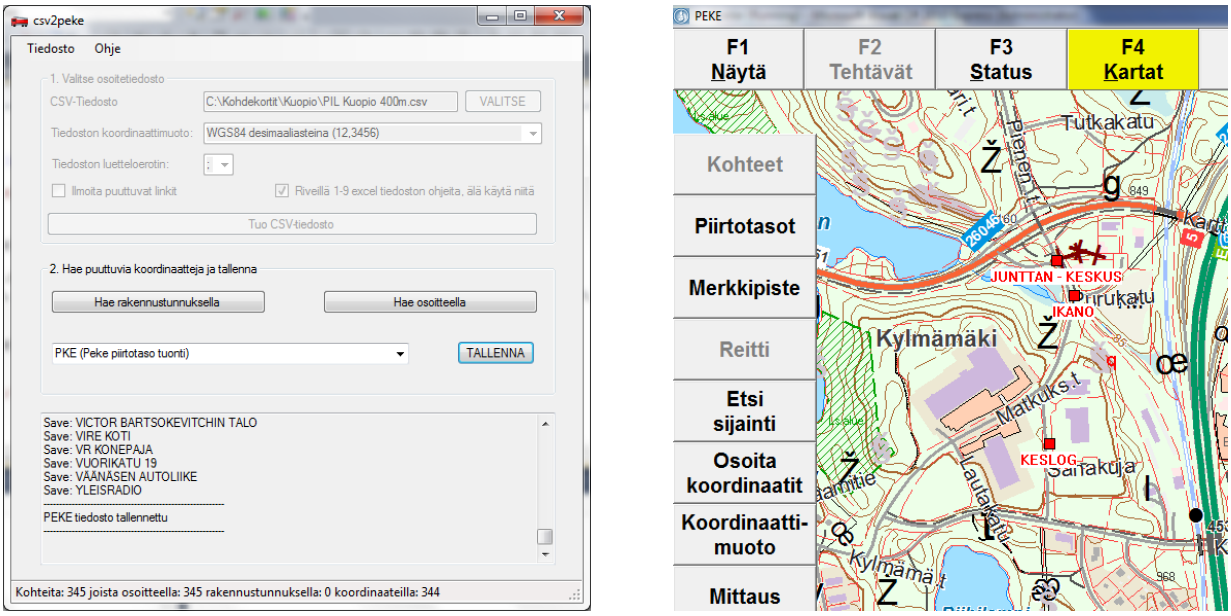
Heti hankkeen alussa lähdettiin rakentamaan myös kehitysympäristöä myös palvelin puolelle PEIP-verkkoon. Palvelimeksi saatiin pelastusopiston omasta käytöstä poistettu HP DL380 G4 palvelin joka on varustettu 180GB RAID5 levystöllä ja kahdennetulla virransyötöllä. Palvelimen prosessori levykapasiteetti ja prosessoriteho ei vastaa tämän päivän tuotantokäytön vaatimuksia, mutta riittää hyvin tuotekehitys ja testaus käyttöön.

Palvelimeen asennettiin ilmainen CENTOS 5.10 Linux käyttöjärjestelmä, MySQL tietokanta ja Apache www-palvelin. Palvelin kytkettiin PEIP-verkkoon ja sijoitettiin pelastusopiston T&K-yksikön laitetilaan.

PEKE karttatasojen luontityökalu

Hankkeen aikana nousi useammassakin keskustelussa esiin tarve saada tuotua mm. kohdetiedot PEKE:n karttanäkymään suurina massoina / listoina. Tätä varten luotiin Windows-ohjelma jolla tuonti voidaan tehdä (kuva 19). Ohjelmalla voidaan lisäksi paikallistaa kohteet osoitteen tai rakennustunnuksen mukaan.

Samaa asiaa oli omalla tahollaan jo selvitellyt Niemisen Marko Päijät-Hämeen pelastuslaitokselta ja luonut alustavan ehdotuksen excel-taulukosta johon siirrettävä tieto kasataan. Ohjelma muutettiin käyttämään Markon määrittelemää formaattia ja sen toiminnallisuus on toistaiseksi Markolla testauksen alla.



Kuva 19 Ohjelma PEKE karttatasojen luontiin

TUPO hanke

Pelastustoimi toimii yhdessä muiden viranomaisten kanssa moniviranomaistilanteissa usein johtovastuussa. Tällaisissa tilanteissa yhteinen tilannekuva ja viranomaisten välinen viestintä vaativat että pelastustoimi voi hyödyntää tulevaisuuden tietojärjestelmiä ja palveluita täydessä mittakaavassa. Olennaisen tärkeää on pystyä hyödyntämään viranomaisten yhteiskäyttöön tuotettuja työkaluja, kuten viranomaisten kenttäjohtamisjärjestelmää KEJOa.

Kuntaviranomaisen toimiessa yhteistoiminnassa valtion viranomaisten kanssa ongelmaksi saattaa muodostua lainsäädännön ja käytänteiden eroavaisuus tietoturvan osalta. Valtion viranomaisilla on selkeästi määritellyt ja vakiintuneet tietoturvapolitiikat. Pelastustoimen osalta tietoturvakriteerit tulevat usein laitoksen isäntäkunnalta joka myös tuottaa suuren osan pelastuslaitoksen tietoteknisestä infrastruktuurista ja palveluista. Tässä tilanteessa on ymmärrettävää että 22 aluelaitoksen osalta tietoturvapolitiikoissa on eroavaisuuksia.

Valtion viranomaista koskeva tietoturva-asetus ei koske kuntaviranomaista ja näin ollen valtion viranomaisen tietoturvapolitiikka on helposti tiukemmin määritelty kuin kuntasektorilla. Tämä aiheuttaa ongelmia tietojärjestelmähankkeissa joissa pelastustoimen tulisi pystyä esiintymään yhtenä, ei 22 viranomaistahona.

Selkeästi on tullut esille, mm. KEJO-projektin tietoturvatyöpajassa, että pelastustoimen tietoturvapolitiikka ja tietoturvaan liittyvät määrittelyt ovat muiden viranomaisten vastaavista jäljessä. Yhteisten tietojärjestelmien ja tietoverkkojen käytön kannalta on olennaisen tärkeää että pelastustoimi saa oman yhteisen, harmonisoidun tietoturvapolitiikan joka mahdollistaa tietoturvatyön muiden viranomaisten kanssa. Ilman tietoturva-asioiden selkeää määrittelyä on erittäin vaikea toimia yhteisissä tietojärjestelmähankkeissa valtion viranomaisten kanssa.

Tähän ongelmaan TUPO hanke lähti hakemaan ratkaisua verkostoitumalla laitosten ICT-asioista vastaavien henkilöiden, valtionhallinnon tietoturvahenkilöiden ja olemassa oleviin ICT-hankkeisiin.

Hankkeen tavoitteet

Hankkeen tavoitteet oli määritelty projektisuunnitelmassa seuraavasti:

- Koota yhteen pelastuslaitosten isäntäorganisaatioiden tietoturvavastaavat
- Koostaa pelastuslaitosten isäntäorganisaatioiden tietoturvapolitiikat
- Analysoida koostetut dokumentit ja löytää yhteneväisyydet ja erot
- Tuottaa tietoturvapolitiikka joka on laitosten isäntäorganisaatioiden hyväksyttävissä
- Jalkauttaa tietoturvapolitiikka laitoksille koulutuksin ja hankkeisiin tiedottamalla

Tietoturvaan liittyvät kysymykset pelastustoimen tietojärjestelmissä

Yhtenä hankkeen selkeänä toimintona oli toimia asiantuntijatehtävissä pelastustoimen tietojärjestelmähankkeissa sekä tarpeen mukaan pelastustoimen tietoturvakysymysten asiantuntijatehtävissä turvallisuusviranomaisten yhteisissä tietojärjestelmähankkeissa. TUPO hanke oli koko hankkeen ajan tiiviissä yhteistyössä VARANTO -hankkeen kanssa määrittelemässä tarvittavia tietoturvamenettelyjä. Tehtyä työtä on kuvattu jo aiemmin tässä raportissa kohdassa VARANTO.

Sähköpostiohjeistus

Selkeäksi ongelmaksi jo hankkeen alkuvaiheessa todettiin suojaustasoluokitellun materiaalin välittäminen eri tahojen välillä. Etenkin valtio-kunta raja aiheuttaa ongelmia erilaisten käytänteiden ja ympäristöjen osalta, kun kuntaviranomainen ei useinkaan ole valmis vastaanottamaan suojaustasoluokiteltua materiaalia esimerkiksi sähköpostitse.

Hankkeen toimesta päätettiin tuottaa ohjeistus suojaustasoluokitellun postin välittämiseen sähköpostitse pelastustoimessa. Tämä ohjeistus nähtiin selkeästi yhdeksi akuuteimmista pelastustoimen tietoturvaohjeistuksista.

Ohjeistuksen laadinnassa lähdettiin liikkeelle ficoran hyväksymistä salausratkaisuista suojaustasoluokitellulle tiedolle. Lähtökohtaisesti tarjolla ollut ratkaisu piti sisällään kassakaapissa säilytettävän päätelaitteen, jota ei kytkettäisi verkkoon. Käytettävyydeltään tällainen ratkaisu nähtiin aivan liian kömpelöksi joten verraten paljon aikaa käytettiin vastaavat suojamekanismit tuottavan teknisen ratkaisun löytämiseksi. Näin ollen ohjeistuksesta tuli kaksiosainen, toisessa osassa ohjeistetaan loppukäyttäjää ja toinen ohje on ylläpidolle. Ylläpidon ohjeistus kuvaa seikkaperäisesti ne toimenpiteet joilla käyttäjän työasema saatetaan sellaiselle tietoturvan tasolle, että sähköpostin ja siellä välitetyn suojaustaso 4 luokitellun materiaalin käsittely on mahdollista.

Ohjeistukset on julkaistu pelastusopiston julkaisusarjassa:

Marko Hassinen: Salassa pidettävän tiedon välittäminen sähköpostitse pelastustoimessa suojaustasolla IV. Ylläpidon ohjeistus.

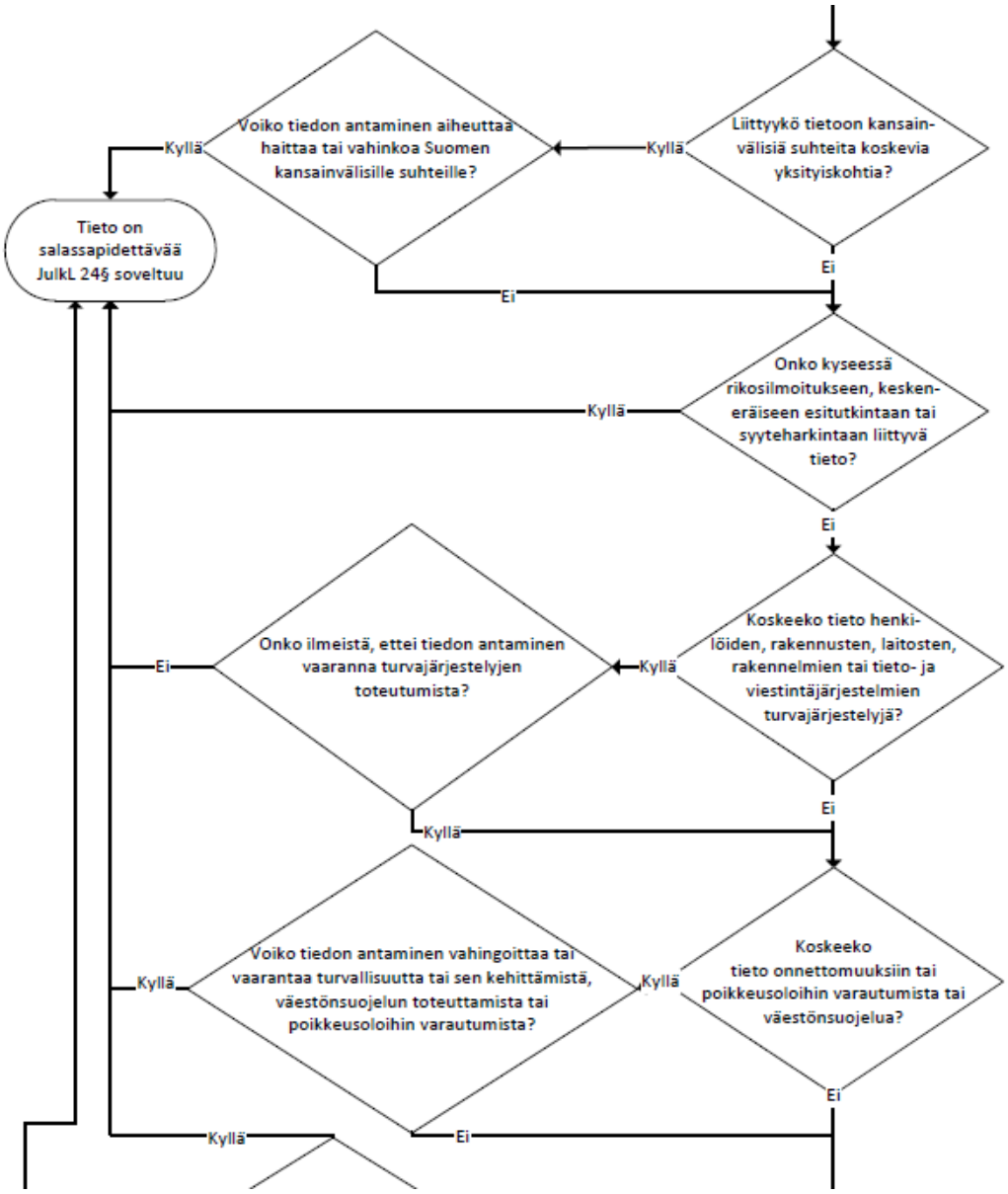
Marko Hassinen: Salassa pidettävän tiedon välittäminen sähköpostitse pelastustoimessa suojaustasolla IV.

Julkaisut ovat vapaasti saatavilla pdf muotoisina pelastusopiston www-sivuilta osoitteesta: http://www.pelastusopisto.fi/fi/tutkimus-_ja_tietopalvelut/kirjasto-_ja_tietopalvelut/julkaisut

Salassapito ja suojaustasoluokittelu pelastustoimessa

Pelastustoimen tietojen luokittelu suojaustasoittain on kuntaviranomaisen kannalta vapaaehtoista. Lainsäädäntö ei luokittelua edellytä, mutta yhteistoiminta muiden turvallisuusviranomaisten kanssa on helpompaa, mikäli luokittelu osataan tehdä ja sitä käytetään sellaisen materiaalin osalta, jota luovutetaan muille viranomaisille. Näin ollen hankkeessa käynnistettiin selvitystyö jonka tavoitteena on tuottaa ohjeistus salassa pidettävän tiedon tunnistamiseen ja suojaustasoluokitteluun pelastustoimessa. Tätä raporttia kirjoitettaessa työ on edelleen käynnissä ja sen uskotaan valmistuvan vuoden 2014 aikana.

Ohjeistuksen kantavana ajatuksena on tuottaa selkeä ja helposti lähestyttävä ohjeistus sinällään varsin laajan ja monitahoisen lainsäädännön pohjalta. Työssä on hyödynnetty mm. vuokaavioita, joihin on tiivistetty pelastustoimen kannalta olennainen lainsäädäntö helposti seurattavaan, loogisesti etenevään kaavioon. Esimerkki tällaisesta kaaviosta on kuvassa 20.



Kuva 20 Vuokaavio tiedon salassa pidettävyyden arviointiin

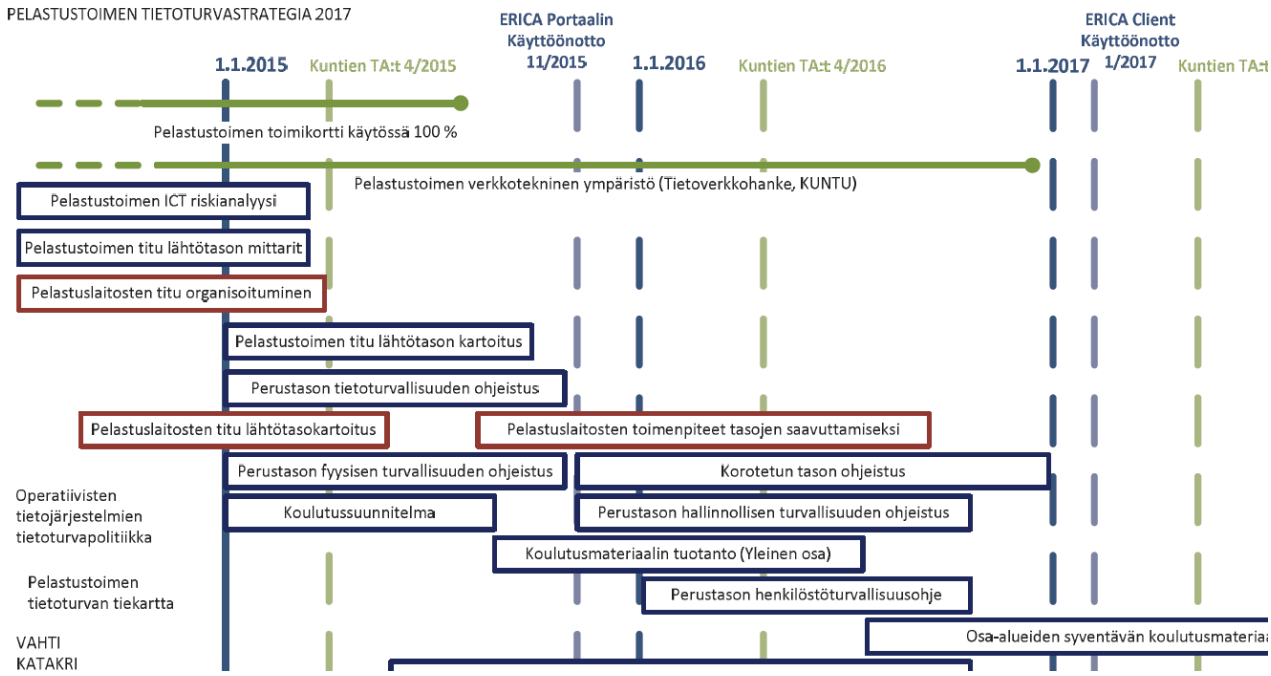
Ohjeistus ilmestyy pelastusopiston julkaisusarjassa, josta se on kaikkien vapaasti saatavilla pdf muotoisena.

Pelastustoimen tietoturvastrategia 2017

Turvallisuusviranomaisten yhteisten tietojärjestelmien käyttöönotossa pelastustoimi on siinä suhteessa erilaisessa asemassa muihin viranomaisiin nähden että pelastustoimen tietoteknisen infrastruktuurin tuottaa yleensä kunnallinen toimija. Näin ollen tietoturvaan kohdistuvien menettelyjen ja määritysten takana ei ole sama lainsäädäntö kuin valtiollisilla toimijoilla ja toimintatavat ovat erilaisia.

Tulevat järjestelmät kuitenkin edellyttävät samanlaisia tietoturvamenettelyjä kaikilta käyttäjiltä, joten kunnallisten toimijoiden on pystyttävä tarjoamaan käyttäjilleen sellaisia ympäristöjä, että ne täyttävät asetetut kriteerit. Tämä aiheuttaa muutostarpeita myös hallintoon, koulutukseen, fyysiseen ympäristöön kuin henkilöstöturvallisuuteen. Hankkeessa keväällä 2014 pidetyssä työpajassa tunnistettiin tarvittavia toimenpiteitä, jotka yllä kerrotusta aiheutuu ja sijoitettiin niitä aikajanalle. Työn tulosta jalostettiin syksyllä 2014 Jyväskylässä pidetyssä työpajassa.

Työnimenä tälle esitykselle on pidetty otsikossa mainittua tietoturvastrategiaa. Esitys on tiivistetty yhteen Gant -kaavioon, josta alla on ote (kuva 21) ja koko kaavio löytyy liitteestä 1.



Kuva 21 Ote pelastustoimen tietoturvastrategia 2017 kaaviosta

Tavoitteena tällä tietoturvastrategialla on tunnistaa toimenpiteet, jotka toimialan on tehtävä vuoden 2017 loppuun mennessä, jotta pelastustoimen toimintaympäristö tyydyttää tulevien tietojärjestelmien vaatimukset. Strategiaa on käsitelty pelastustoimen tietoteknisiä hankkeita koordinoivassa ryhmässä (PTK) sekä pelastusjohtajien kokouksessa, joka suosittaa pelastuslaitoksia ottamaan ohjeen käyttöön.

Pelastustoimen operatiivisten tietojärjestelmien tietoturvapolitiikka

Kun yhtenä tavoitteena oli koota yhteen pelastuslaitosten tietoturvavastaavat, huomattiin, ettei tämä onnistu siitä syystä, ettei monellakaan laitoksella ole nimettynä tällaista henkilöä. Yleisesti tietoturvaan liittyvä ohjeistus ja neuvonta, kuten myös määräykset, tulevat isäntäorganisaatiosta tai sen käyttämältä palveluntarjoajalta.

Tietoturvapolitiikkaan tämä kuitenkin kirjattiin siten että jokaisella laitoksella olisi tietoturvasta vastaava henkilö. Hankkeen näkemyksen mukaan tämä on tulevaisuudessa lähestulkoon välttämätöntä, mutta ei tarkoita sitä että tietoturvavastaavan tulisi hoitaa tätä tehtävää päätoimisesti.

Vaikka hankkeen tavoitteena oli tuottaa tietoturvapolitiikka vain operatiivisiin tietojärjestelmiin, tuli kahden isännän ongelma vahvasti esiin. Pelastuslaitosten tietoturvalinjaukset tulevat vahvasti isäntäorganisaatioista, eikä pelastustoimea koko maan laajuisena toimijana edusta kukaan tai mikään taho. Näin ollen pelastustoimea kokonaisuutena ohjaavan tietoturvapolitiikan mandaatti on vaikea asettaa mihinkään. Pelastustoimen kumppanuusverkostolla on roolinsa koko maan pelastustoimea ohjaavana orgaanina, mutta määräysvalta on luonnollisesti isäntäorganisaatioissa.

Ensimmäinen versio joka hankkeen aikana jäi myös viimeiseksi, on tämän raportin liitteessä 2. Kyseisestä dokumentista saatiin pelastuslaitokselta sinällään yllätyksettömät kommentit, joiden viesti on edelliseen kappaleeseen jo kirjoitettukin.

Kun kesken hankkeen saatiin tieto KUNTU -hankkeesta ja sen sisällöstä saatiin jonkinlainen kuvaus, todettiin sillä olevan oma vaikutuksensa mahdolliseen pelastustoimen yhteiseen operatiivisten tietojärjestelmien tietoturvapolitiikkaan. Näin ollen tietoturvapolitiikan määrittely jäin jossain määrin taka-alalle ja hankkeessa keskityttiin muihin tärkeisiin kohteisiin. KUNTU -hankkeen suunnitteluvaiheesta ei kuitenkaan saatu TUPO -hankkeen päättymiseen tai tämän raportin kirjoittamiseen mennessä mitään tietoa joten sen vaikutuksia on mahdoton arvioida. Joka tapauksessa, tietoturvapolitiikkaan on syytä palata siinä vaiheessa kun KUNTUsta saadaan jotain konkreettista tietoa.

Yhteenveto

VOTI -hankkeen pilotti arvioitiin selkeästi onnistuneeksi ja se täytti käyttäjien tarpeet hyvin. Työtä konseptin rakentamisessa jäin luonnollisesti hankkeen jälkeen runsaasti tehtäväksi, pääosin hankkeesta riippumattomista syistä. Nykyisestä pilotista saatavat kokemukset antavat suuntaa jatkokehitykselle ja tunnistaa sellaisia tarpeita, joita hankkeen aikana ei tullut esiin.

Olennaista pelastustoimen operatiivisessa työasemainfrastruktuurissa on saada aikaan sellainen konsepti jota koko suomen pelastustoimi voi käyttää, sen sijaan että tätä samaa työtä tehtäisiin jokaisella laitoksella erikseen. Tällä tavoin voidaan saavuttaa todellisia kustannussäästöjä ja helpottaa työntekijöiden päivittäisiä työtehtäviä. Yhtenäiset menettelyt ja ympäristöt myös helpottavat yhteistoimintaa ja henkilöstön liikkuvuutta.

Työasemakonseptin kehittäminen ei kuitenkaan riitä pitkällä aikavälillä, vaan ympäristöt vaativat myös ylläpitoa, eikä tätä työtä voi juurikaan rakentaa hanketoiminnan varaan.

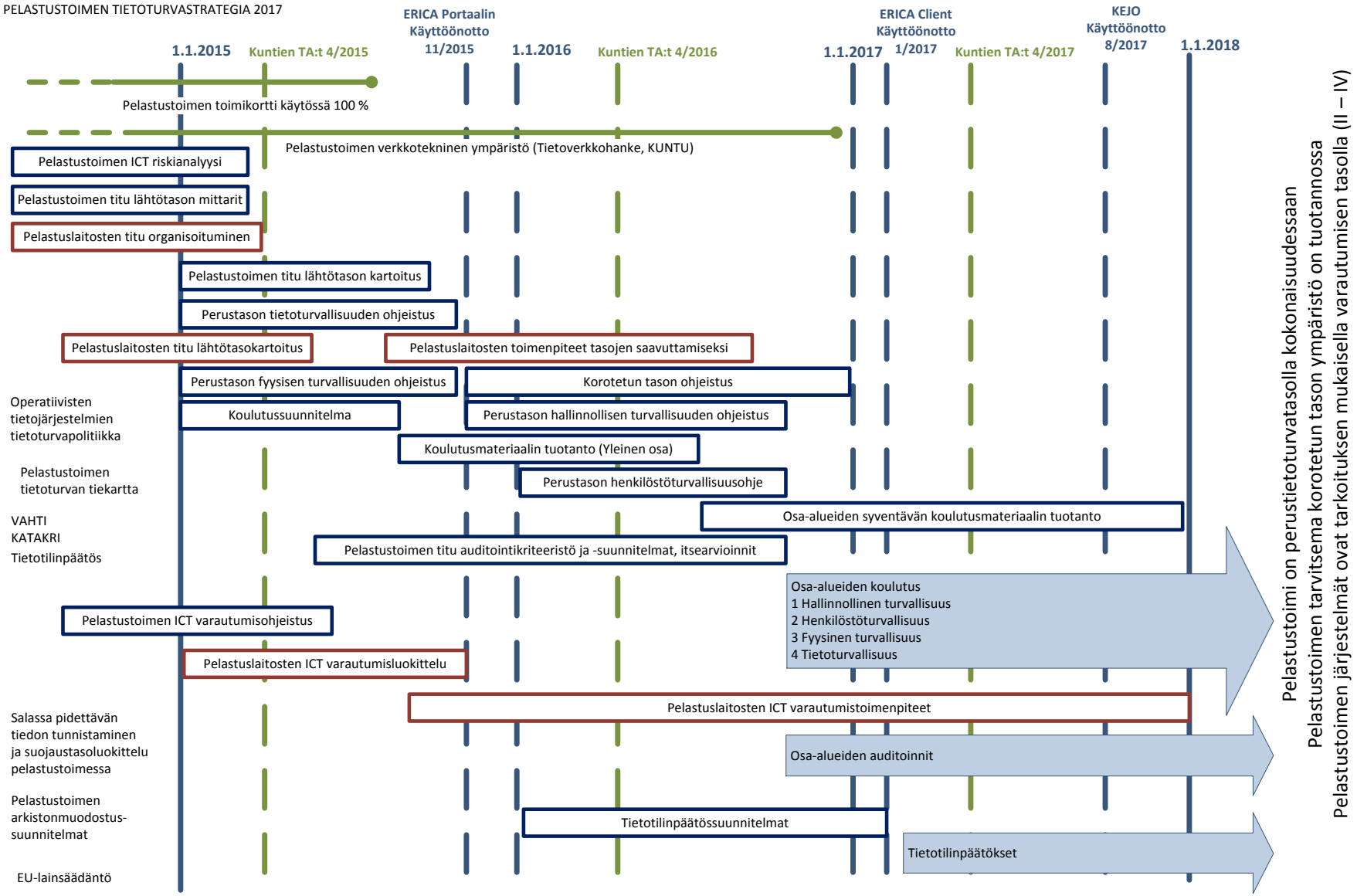
TUPO hankkeen aikana pelastustoimen tietoturvakysymyksiä käsiteltiin hyvin monipuolisesti ja hankkeen toimesta laadittiin useampia ohjeistuksia. Hankkeessa aloitetuista ohjeistuksista useiden työstämistä myös jatketaan hankkeen päätyttyäkin hankkeessa luotujen verkostojen toimesta.

Pelastustoimen tietoturvakysymysten ratkaiseminen akutisoituu lähivuosina uusien, viranomaisten yhteisten tietojärjestelmien tietojärjestelmien tullessa käyttöön. Näiden tietojärjestelmien myötä pelastustoimeen kohdistuu uusia tietoturvavaatimuksia, joita ei ole aiemmin ollut.

TUPO hankkeessa käytiin läpi pelastustoimen tulevaisuuden tietoturvatarpeita ja rakennettiin Pelastustoimen tietoturvastrategia 2017. Strategiassa määritettiin sellaiset toimenpiteet, jotka tarvitaan tehdä jotta pelastustoimi on valmis viranomaisten yhteisiin tietojärjestelmiin.

Itse tietoturvapolitiikasta laadittiin lausuntoversio, josta saatiin pelastuslaitokselta palautetta. Vaikka kyseessä oli vain operatiivisiin tietojärjestelmiin kohdistuva tietoturvapolitiikka, tuli isäntäorganisaatioiden ohjausrooli selkeästi esille ja sen sitovuutta korostettiin. Samaan aikaan alkanut KUNTU hanke osaltaan tulee vaikuttamaan operatiivisten järjestelmien tietoturvan ohjaukseen ja TUPO hanke keskittyi muihin tärkeisiin tietoturvakysymyksiin, kuten yllä mainittuun tietoturvastrategiaan. Kun KUNTU hankkeesta saadaan tuloksia, on aika uudelleen arvioida tietoturvapolitiikan merkitystä ja sen mahdollisuutta tulla toimialalla hyväksytyksi.

LIITE 1 Tietoturvastrategia 2017



Pelastustoimen operatiivisten tietojärjestelmien tietoturvapolitiikka

Marko Hassinen

Pelastusopisto

Pelastusopiston julkaisu

D-Sarja: Muut julkaisut

2014

ISBN EI JULKAISTU

ISSN EI JULKAISTU

PELASTUSOPISTO

Pelastustoimen operatiivisten tietojärjestelmien tietoturvapolitiikka

Hassinen Marko, FT, Pelastusopisto, Tutkimus- ja kehittämisyksikkö

Elokuu 2014

TIIVISTELMÄ

EMERGENCY SERVICES COLLEGE

Data Security policy for Fire & Rescue operative data systems

Hassinen Marko, Ph.D., Emergency Services College, R&D unit

Research report XX pages, X attachments (x pages)

August 2014

ABSTRACT

JOHDANTO

Tässä dokumentissa määritellään Pelastustoimen operatiivisten tietojärjestelmien tietoturvapolitiikka.

Tietoturvapolitiikassa määritellään ne periaatteet ja vastuut, joita pelastustoimen operatiivisissa järjestelmissä noudatetaan tietoturvan määrittelemisessä, kehittämisessä, ylläpidossa, valvonnassa ja raportoinnissa. Tietoturvapolitiikkaa täydentävät yksityiskohtaisemmat tietoturvaohjeet määritellään erikseen.

MITÄ OVAT TIETOTURVA JA SEN TAVOITTEET

Tietoturvan tavoitteena on varmistaa pelastustoimen operatiivisten tietojärjstelmien toimintakyky ja -varmuus ja siten osaltaan varmistaa pelastustoimen kyky tuottaa siltä edellytettyjä palveluja. Tietoturva osaltaan myös takaa toimintojen jatkuvuuden ja organisaation toimintakyvyn jatkuvuuden niiltä osin kuin se perustuu operatiivisiin tietojärjestelmiin.

Tietoturvan kolme olennaista tavoitetta ovat

Saatavuus: Tieto on aina siihen oikeutetun tahon saatavilla

Eheys: Tieto ei muutu tai tuhoudu tarkoituksettomasti

Luottamuksellisuus: Salassa pidettävä tieto on vain tietoon oikeutettujen saatavilla

Tietoturvalla tavoitellaan pelastustoimea aina, kaikissa tilanteissa tarkoituksen mukaisella tavalla palvelevia operatiivisia tietojärjestelmiä.

TIETOTURVAN KEHITTÄMINEN JA VALVONTA

Tietoturvaa täytyy jatkuvasti muuttuvassa ympäristössä kehittää jotta se ajan tasaisesti suojaa organisaatiota ja sen toimintakykyä.

Olennaisin osa tietoturvaa ovat järjestelmien käyttäjät, joten pelastustoimi aktiivisesti kouluttaa henkilöstöään tietoturvamenettelyiden osalta. Henkilöstöä myös jatkuvasti tiedotetaan tietoturvaan liittyvissä muutoksissa. Jokainen henkilö on saanut riittävän perehdytyksen tietoturvaan liittyvissä asioissa.

Pelastustoimi jatkuvasti analysoi toimintaansa kohdistuvia tietoturvariskejä ja seuraa muiden viranomaisten sekä yritysten tietoturvatiedottamista.

Pelastuslaitoksilla tietoturvatasoa, tietoturvariskejä sekä tietoturvakoulutuk-sen tarvetta valvoo tietoturvavastaava.

FYYSINEN TURVALLISUUS

Tietoturvallisuuden yhtenä lajina fyysisen turvallisuuden varmistaminen on tärkeää pelastustoimen operatiivisten tietojärjestelmien sisältämän tiedon luottamuksellisuuden varmistamisessa. Jokainen pelastustoimen operatiivisia järjestelmiä käyttävä henkilö on ohjeistettu fyysisen turvallisuuden osalta.

Fyysisellä turvallisuudella tarkoitetaan sitä, ettei luvattomilla henkilöillä ole pääsyä tiloihin joissa käsitellään operatiivisia tietojärjestelmiä (mukaan lukien ajoneuvot). Pelastuslaitosten tiloissa on asianmukaiset kulunvalvontamenettelyt.

TIETOJEN LUOTTAMUKSELLISUUS

Pelastustoimen tietojen luottamuksellisuutta säätelee muun muassa Laki viranomaisen toiminnan julkisuudesta. Pelastustoimen henkilöstö on koulutettu tunnistamaan salassa pidettävä tieto ja käsittelemään salassa pidettävää tietoa oikein. Pelastustoimessa viranomaisen asiakirjatieto luokitellaan suojaustasoluokitusta käyttäen.

Käyttöoikeus salassa pidettävään tietoon on rajattu tehtävän mukaisesti. Salassa pidettävän tiedon käyttöä valvotaan tietojärjestelmän toimesta. Salassa pidettävää tietoa haltuunsa saanut henkilö on velvollinen käsittelemään tietoa siten ettei se päädy ulkopuolisen tietoon.

Tiedon elinkaaren päätyttyä tieto hävitetään luotettavasti.

TIETOJÄRJESTELMÄT JA SÄHKÖPOSTI

Pelastustoimen operatiivisia tietojärjestelmiä käytetään operatiivisen toiminnan hoitamiseen. Tietoliikenneyhteydet ja sähköposti ovat työtehtävien hoitamista varten.

Sähköpostin käyttöön on oma ohjeistuksensa ja jokaisen henkilön tulee tuntea tämä ohjeistus. Salassa pidettävän materiaalin välittämiseen sähköpostitse on ohjeistus, jonka mukaan jokaisen on toimittava käsitellessään salassa pidettävää materiaalia sähköpostitse. Sähköposti nauttii kirjesalaisuuden suojaa.

TIETOTURVAOHJEISTUS

Tietoturvaohjeiden laadinnasta ja ylläpidosta vastaa pelastuslaitosten kumppanuusverkoston tietoturvallisuuden johtoryhmä. Ohjeistuksissa kuvataan tavat, joilla toimien työntekijä minimoi tietoturvariskejä. Jokaisen työntekijän tulee noudattaa annettuja ohjeistuksia.

ORGANISOINTI JA VASTUUT

Ylätason vastuu tietoturvan toteutumisesta on pelastusjohtajien hallituksella, jonka tehtävänä on luoda riittävät edellytykset tietoturvan toteuttamiseen.

Pelastuslaitosten kumppanuusverkoston tietoturvallisuuden johtoryhmä vastaa tietoturvan käytännön toimien koordinointi, poikkeamien käsittelystä ja riskien sekä tietoturvan tason riittävyyden tarkastelusta.

Jokaisella pelastuslaitoksella on tietoturvavastaava jonka vastuulle kuuluu laitostason seuranta ja raportointi sekä tietoturvamenettelyjen käyttöönotto.

Jokaisen pelastuslaitoksen toimipisteen esimies vastaa tietoturvaohjeistuksen noudattamisesta toimipisteensä tietojenkäsittelyssä.

SIDOSRYHMÄT JA YHTEISTYÖKUMPPANIT

Tietoturva pyrkii varmistamaan että kanssakäynti sidosryhmien ja yhteistyökumppanien kanssa on sujuvaa ja siihen liittyvät riskit ovat mahdollisimman pienet. Kaikki tahot, joilla on pääsy tavalla tai toisella pelastustoimen operatiivisiin tietojärjestelmiin, sitoutuvat noudattamaan tätä tietoturvapolitiikkaa sekä siihen liittyviä ohjeita.

POIKKEUSMENETTELY

Pelastustoimen operatiivisten tietojärjestelmien tietoturvapolitiikasta tai siihen liittyvästä ohjeistuksesta poikkeava menettely vaatii poikkeusluvan jonka hyväksyy pelastusjohtajien hallitus.

HYVÄKSYMISMENETTELY

Pelastustoimen operatiivisten tietojärjestelmien tietoturvapolitiikan hyväksyy pelastusjohtajien hallitus. Erilliset tietoturvaohjeet ja niiden muutokset hyväksyy pelastuslaitosten kumppanuusverkoston tietoturvallisuustyöryhmä.