TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Määräys 72 työpajat 2020-2021

Määräys 72 A/2018 M sähköisistä tunnistus- ja luottamuspalveluista

Määräys 72 työpajat 2020-2021
Työpaja 4/7 agenda 10.3.2021 klo 9-11.30

- Yleistä: Työpajat, aikataulu, työtapa
  - 1 muutos työpaja-aikatauluun, mahdollinen 21.4. -> 22.4.2021
- 9- n.10.40
- Tunnistusmenetelmä
  - muutosehdotukset
  - PSD2 –vertailu - toimialan mahdolliset havainnot
- *Tauko*
- 10.45-11.30
- SSI, Blockchain
  - Findy –hankkeen esitys
- Seuraava työpaja 15.4.2021: luottamuspalvelut

10.3.2021 työpajan osallistujat

- Työpajassa oli paikalla 25 henkilöä seuraavista organisaatioista
- Aktia, Danske Bank, Handelsbanken, Nordea, OP, POP-pankit, S-pankki, Säästöpankit, Ålandsbanken
- Telia
- Nixu
- Samlink, Ubisecure
- Ficom, FA
- DVV, Fiva, KKV, Puolustusvoimat
- TietoEvry (Findyn edustajana)

Työpajat

16.12.2020-10.6.2021

Työtapa

- Työpajat ovat avoimia sidosryhmille
- Kutsu viimeistään 1-2 viikkoa ennen työpajaa viraston sähköpostijakeluilla (luottamusverkosto, eidas-tekninen, eidas-yleinen ”tulu”)
- Kutsun kanssa samaan aikaan jaetaan/julkaistaan viraston valmistelumuistio työpajan aiheesta
- Työpajoissa käydään läpi valmistelumuistion muutosehdotukset ja niiden vaikutusten arviointi
- Viimeisessä työpajassa käydään läpi koko muutettu määräys ja perustelumuistio
- Sidosryhmät voivat koko työn ajan toimittaa kirjallisia kommentteja valmisteluun. Kommenttien julkisuus arvioidaan julkisuuslain mukaisesti.
- Virasto voi pyynnöstä järjestää kahdenvälisiä tapaamisia asioissa, joita ei voi niiden luonteen takia käsitellä julkisessa työpajassa

Määräystyöpajojen aikataulu

Aika	Materiaali	Aihe	Lisätyöpaja (tarvittaessa)
KE 16.12.2020 9-11.30	7.12.2020	Tunnistus: rajapinnat ja attribuutit	KE 3.2.2021 9-11
KE 20.1.2021 9-11.30	11.1.2021	Tunnistus: Salaus, osapuolten varmentaminen ja avaintenvaihto	KE 3.2.2021 9-11
KE 10.2.2021 9-11.30	1.2.2021	Tunnistus: tunnistusjärjestelmän tekniset vaatimukset ja arviointi	KE 17.2.2021 9-11
KE 10.3.2021 9-11.30	**1.3.2021**	**Tunnistus: tunnistusmenetelmä, PSD2-vertailu Blockchain ja SSI**	KE 17.3.2021 9-11
KE 15.4.2021 9-11.30	1.4.2021	Luottamuspalvelut: palveluiden ja arvioinnin ETSI-standardit	~~KE 21.4.2021~~ TO 22.4. 9-11
KE 12.5.2021	3.5.2021	Tunnistuspalvelun vaatimukset: kooste muutosehdotuksista	TO 20.5.2021 9-11
TO 10.6.2021 9-11.30	3.6.2021	Koko määräys ja perustelut	

Jatkoaikataulu – muutokset mahdollisia

- 6-8/2021 virkavalmistelu ja käännökset
- **9/2021 lausuntokierros**
- 10/2021 lausuntokooste, mahdolliset muutokset ja niiden käännökset
- **10/2021 palautetilaisuus lausuntokierroksen tuloksista**
- n. 10 – 12/2021 määräyksen EU-notifointi
- n. 1-2/2022 uusi määräys voimaan

Määräyspäivityksen yleiset linjaukset

Määräyspäivityksen yleiset linjaukset

- Määräyksen perusrakenne ja lukujako säilytetään
- Vaatimuksia ja perusteluja selvennetään ja ajantasaistetaan joiltain osin
- Viraston ohjeet ja suositukset pääpiirteissään samoissa asioissa kuin nyt
- Muutoksia harkitaan: attribuutit, salausvaatimukset ja luottamuspalveluiden standardiviitteiden täydennykset
  - mm. uhkat perusteena
  - Lisäys 10.3.2021: tunnistusmenetelmän turvallisuusvaatimusten tarkentamista harkitaan
- Operatiivisia palveluita ei ole säädetty viranomaiselle tehtäväksi (vrt. .FI)
- PSD2-vaatimuksia tarkastellaan referenssinä tunnistusmenetelmän vaatimusten kohdalla (nostoja toimijoilta tarvitaan)
- Blockchain: tilaisuus käsitellä lohkoketjuteknologian suhdetta tunnistuksen teknisiin vaatimuksiin ja arviointivaatimuksiin

Tunnistus: tunnistuspalvelun tietoturvavaatimukset

M72 Luku 2 Tunnistuspalvelun tietoturvavaatimukset

6 § Tunnistusmenetelmän tietoturvavaatimukset

Voimassa oleva säännös
6 § Tunnistusmenetelmän tietoturvavaatimukset

Tunnistusvälinettä ei saa yhdistää hakijaan ennen hakijan ensitunnistamista tai tunnistusvälineen myöntämisprosessissa on muutoin varmistettava, että tunnistusväline ei ole käytettävissä ennen kuin tunnistus- ja luottamuspalvelulain 17 §:n mukainen ensitunnistaminen on tehty.

Palveluntarjoajan on varmistettava, etteivät tunnistusvälineeseen liittyvät salaiset tiedot paljastu sen henkilöstölle missään tilanteessa.

Palveluntarjoaja ei saa kopioida tunnistusvälineeseen liittyviä salaisia tietoja.

Muutosehdotus: kohta 6.1 Todentamistekijöiden turvallisuus ja riippumattomuus

6.1 Todentamistekijöiden turvallisuus ja riippumattomuus

Hallussapitoon, tietoon ja ominaisuuteen perustuvien todentamistekijöiden **eri turvaominaisuuksien** ja tunnistusmenetelmän **turvallisuustoimenpiteiden** yhdistelmän on **suojattava** tunnistusmenetelmää oikeudettomalta käytöltä. Todentamistekijöiden **riskit on arvioitava** erikseen ja tunnistusmenetelmän suojautumiskyvyn on perustuttava varmuustason mukaiseen uhka- ja riskiarvioon.

Tunnistusmenetelmän toteutuksen on estettävä se, että yhden todentamistekijän vaarantuminen vaarantaa muiden todentamistekijöiden luotettavuuden. Tunnistusmenetelmän turvatoimenpiteillä on **eriytettävä** ja suojattava todentamistekijät erityisesti, kun niitä käytetään samalla päätelaitteella.

Siirtymäsäännös (?): riskiarvio menetelmästä laadittava x mennessä, uusilla toimijoilla aloitusilmoituksen yhteydessä.

Muutosehdotus: kohta 6.1 Miten määritellään turvalliset tai turvattomat todentamistekijät ja tunnistusmenetelmän kokonaisuus?

a) Määräyksen tarkennetut todentamistekijäkohtaiset vaatimukset?

- ✓ Paljon yksityiskohtia, koska todentamistekijät ovat muuttuvia ja moninaisia

b) Suojautumiskyvyn/lopputuloksen määrittely?

- ✓ Hyökkäyksensietokyky kohtuullisen tai korkean kyvykkyystason hyökkäyskykyä vastaan säädetään laissa ja varmuustasoasetuksessa, mutta mahdollisesti tarkennettavissa
- ➢ Hallussapitoon, tietoon ja ominaisuuteen perustuvien todentamistekijöiden eri turvaominaisuuksien ja tunnistusmenetelmän turvallisuustoimenpiteiden yhdistelmän on suojattava tunnistusmenetelmää oikeudettomalta käytöltä.

c) Riskiarvion vaatimukset?

- ✓ Nyt harkinnassa oleva malli on tarkentaa määräyksessä tätä, koska malli on joustava eri tunnistusmenetelmien ja todentamistekijöiden suhteen
- ➢ Todentamistekijöiden riskit on arvioitava erikseen ja tunnistusmenetelmän suojautumiskyvyn on perustuttava varmuustason mukaiseen uhka- ja riskiarvioon.
- ▶ *LOA guidance: eri tekijät on valittava niin, että niillä torjutaan eri uhkia/hyökkäystapoja*
- ▶ *LOA guidance: on syytä ottaa huomioon paitsi itse tekijä tai tekijät, myös tekijöiden varmentamisessa käytettävä menettely*

Muutosehdotus: kohta 6.1 Todentamistekijöiden riippumattomuus

- Tunnistusmenetelmän toteutuksen on estettävä se, että yhden todentamistekijän vaarantuminen vaarantaa muiden todentamistekijöiden luotettavuuden. Tunnistusmenetelmän turvatoimenpiteillä on eriytettävä ja suojattava todentamistekijät erityisesti, kun niitä käytetään samalla päätelaitteella.
- Vrt. PSD2 RTS SCA&CSC 9 artikla Tekijöiden riippumattomuus toisistaan

  1. ...varmistettava, että...tekijöihin sovelletaan toimenpiteitä, joilla varmistetaan teknologian, algoritmien ja parametrien osalta, ettei yhden tekijän rikkominen aseta kyseenalaiseksi muiden tekijöiden luotettavuutta.

  2. ...toteutettava turvatoimenpiteitä, joita sovelletaan...tekijää tai itse tunnistamiskoodia käytetään monikäyttölaitteella, ja joilla vähennetään monikäyttölaitteen vaarantumisesta aiheutuvaa riskiä.

  3. ...riskinhallintatoimenpiteiden on sisällettävä...:

  a) erillisten suojattujen toteuttamisympäristöjen käyttö monikäyttölaitteeseen asennetun ohjelmiston välityksellä;

  b) mekanismit, joilla varmistetaan, ettei maksaja tai kolmas osapuoli ole muuttanut ohjelmistoa tai laitetta;

  c) jos muutoksia on tapahtunut, mekanismit, joilla lievennetään niiden seurauksia.
- Vrt. tunnistuspalvelun arviointiohjeen 211/2019 mobiilisovelluskriteeristö

Muutosehdotus: kohta 6.1 soveltaminen, riskiarviomalli

- Valmistelumuistiossa riskiarviointisapluuna
  - Koottu uhkia mm. varmuustasoasetuksen LOA guidancesta
  - Huom. liikennevaloarviot esimerkkejä
- Uhka/riskiarvio

  todentamistekijäkohtainen uhka/riskiarvio, ml. riippumattomuus

  +todentamismekanismin uhka/riskiarvio

  + havainnot toteutuneista riskeistä

  +turvakontrollit em. vastaan

  =kokonaisarvio
- Sapluunan laatiminen? Reunaehdot/suuntaviivat määräyksen perusteluihin, muuta?
- Vaikutukset
  - Osa perusluonteista toimintaa, mutta mahdollisesti tarkentaa ja lisää dokumentointia
- Valvonta
  - Esim. tunnistusmenetelmän muutosten yhteydessä, määräaikaisarvointien yhteydessä, mahdollisesti erillinen seuranta määräyksen antamisen jälkeen
  - Viranomaisen mahdollinen puuttuminen riskiarvion perusteella tarjottuun menetelmään perustuu häiriökäyksensietokyvyn arvion kokonaisuuteen

Kommentit työpajassa 10.3.2021/todentamistekijöiden turvallisuus ja riippumattomuus

- Kysyttiin, mitä tarkoitetaan *erillisellä seurannalla* määräyksen antamisen jälkeen ja onko mahdollista liittää riskiarviointi mukaan määräaikaisarviointeihin?
  - Traficom: Seuranta tarkoittaa yleensä kirjallisia valvontakyselyitä, joilla toteutusta seurataan. Yritetään lähtökohtaisesti yhdistää mahdollisimman paljon määräaikaisarviointien yhteyteen.
- Riskilähtöinen lähestymistapa koettiin positiiviseksi, mutta kommentoitiin, että viraston valvonnan kannalta on tärkeää ohjeistaa mitä arvioidaan ja millä metodilla. Jäännösriskin hyväksyttävyydestä voi olla erilaisia näkemyksiä viraston ja tunnistuspalveluiden välillä.
  - Traficom: pyritään ennakoimaan vähimmäisvaatimusten määrittelyä ja mahdollistamaan ennestään käytettyjen arviointien hyödyntäminen.
  - Fiva kertoi, että EBA:lta on tullut joitain uusia Q&A vastauksia, jotka voisi lisätä lähteisiin. Fiva toimittaa virastolle erikseen. Toinen koski yhteiskäyttölaitteita joista EBA totesi, että ei ole esteitä että tunnistussovelluksessa on eri käyttäjäprofiileja. Toinen kysymys koski etäyhteyttä laitteeseen, jossa tunnistussovellus sijaitsee ja sitä, miten hallussapitoelementti pitää tulkita.
  - Todettiin yhteisesti, ettei riskiarviointiin tarvita määräyksessä siirtymäaikaa.
  - Traficom: ei aikomusta asettaa arvioinnille tiettyä pakollista vakiomuotoa, mutta vähimmäisvaatimuksia otetaan perusteluihin mukaan. Ennestään käytössä olevia riskiarviomenetelmiä voi hyödyntää, eikä esim. englannin kieli ole ongelmallinen.
  - Ehdotettiin, että ISO31000-standardit ja VAHTI-arviointiohje voivat olla hyödyllisiä riskiarvioinnin laatimisessa.
- Keskusteltiin, olisiko tarvetta erilliselle rekisterille ja keskustelulle jo huomatuista riskeistä ja ongelmista, joita yrityksillä on tullut vastaan? Voisiko tietoa jakaa anonyymisti ja näin parantaa yhdessä tietoturvaa yleisellä tasolla? Kommentoitiin, että kynnys jakaa luottamuksellista tietoa on korkea, sillä riskienhallinta on osa liiketoimintaa. Osa riskeistä on samanlaisia, mutta niihin sisältyy paljon yksityiskohtia ja riskin olennaisuuden merkitys vaihtelee eri organisaatioiden välillä. Se miten riskeihin voidaan vaikuttaa, on yrityksen omaa harkintaa.
  - Traficom: tarkastellaan asiaa luottamusverkoston yhteistoimintaryhmän häiriötiedon vaihdossa.

Muutosehdotus 6.2 Todentamismekanismin turvallisuus

6.2 Todentamismekanismin turvallisuus

Käyttäjän tunnistusvälineen ja tunnistusvälineen/palvelun tarjoajan järjestelmän välisen tietoliikenneturvallisuuden tulee täyttää soveltuvin osin määräyksen 7 kohdan [ja 9 kohdan] salausvaatimukset.

Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto, jonka perusteella käyttäjä voi varmistua siitä, että hän vahvistaa oikean tunnistuspyynnön (session binding). Tieto on näytettävä tunnistusmenetelmässä, jossa se on teknisesti mahdollista.

Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto luottavasta osapuolesta, jolle tunnistus välitetään. Tieto on näytettävä tunnistusmenetelmässä, jossa se on teknisesti mahdollista. (RP-name)

Muutosehdotus 6.2 Todentamismekanismin turvallisuus/salaus, istunnon kesto

- Salaus
  - Tarkkaa arviota ei vielä ole, mutta tarkoitus on, että nykyisen määräyksen 7 §, 8 § ja 9 § kokonaisuus katetaan
  - Arvioitava vielä kokonaisuutena määräykseen 7 kohdan ja 9 kohdan kanssa
  - todentamismekanismissa noudatetaan salausvaatimuksia tunnistusvälineen tarjoajan ja käyttäjän välillä
  - sanomat/viestit tunnistusvälineen käyttäjän ja IdP:n välillä
- Huomioita?
- lisäksi istunnon kesto?
  - Vrt. rajapintasuositus 212 ja 213

Muutosehdotus 6.2 Todentamismekanismin turvallisuus/session binding

- Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto, jonka perusteella käyttäjä voi varmistua siitä, että hän vahvistaa oikean tunnistuspyynnön (session binding). Tieto on näytettävä tunnistusmenetelmässä, jossa se on teknisesti mahdollista.
- Turvallisuus- ja kehitystavoite:
  - sitoa/yhdistää selain/sovellusistunto tunnistustapahtumaan, session binding
  - tunnistuspalvelun arviointikriteeristössä vaatimuksena mobiilisovellukselle
- Toteutettavuushuomioita
  - tunnistuspyynnön yksilöinti
  - tunnistusvälineen käyttöliittymässä => mahdollinen vain tunnistusvälineessä, jolla on oma näyttö
  - Erilaisia vertailutietoja, merkkijono, QR-koodi, kuvia
- Muita huomioita?

Muutosehdotus 6.2 Todentamismekanismin turvallisuus/RP-name

- Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto luottavasta osapuolesta, jolle tunnistus välitetään. Tieto on näytettävä tunnistusmenetelmässä, jossa se on teknisesti mahdollista. (RP-name)
- Turvallisuus- ja kehitystavoite
  - Käsitelty attribuuttivelvoitteiden kohdalla
- Toteutettavuus
  - Tieto kohdepalvelusta (SP/RP –name) tulossa pakolliseksi attribuutiksi
  - tunnistuspalvelun (välityspalvelun ja/tai välineen tarjoajan) käyttäjälle tarjoamassa selain-käyttöliittymässä ja mahdollisesti tunnistussovelluksessa
- Muita huomioita?

Kommentit työpajassa 10.3.2021 /todentamismekanismi

- Salauksesta ja istunnon kestosta ei kommentteja.
- Kommentoitiin, että esimerkiksi mobiilivarmenteissa harvat käyttäjät aktivoivat vapaaehtoiset lisäturvatekijät
- Kommentoitiin, että session binding on tietoturvaa parantava ominaisuus, mutta toimivuus riippuu siitä, miten se toteutetaan.
- Toteutettavuuden osalta toivottiin, että jätetään jokaisen organisaation päätettäväksi ja viraston tehtäväksi jää arvioida toteutuksen toimivuus.
- Traficom pyysi näkemyksiä, voidaanko binding message ottaa velvoittavaksi mukaan määräykseen ja onko tarvetta siirtymäajalle?
  - Kommentoitiin, että binding messagen vaikutus turvallisuuteen riippuu tunnistusvälineen koosta. Ne toimijat, kenelle tämä on kriittinen ominaisuus, ottavat varmasti nopeasti käyttöön.
  - Traficom totesi yhteenvetona, että otetaan määräystason vaatimukseksi, mutta ei määrätä tiettyä toteutustapaa.
  - Täydennys 26.3.2021: siirtymäajan tarpeellisuus jäi vielä kokonaisuutena epäselväksi.
- Kommentoitiin samassa yhteydessä vastuunjakautumisesta kuluttajan ja organisaation välillä tietoturvan toteuttamisessa. Tietoturvaan liittyviä valintoja ei voi jättää pelkästään kuluttajan vastuulle, joka yleensä arvioi riskin mahdollisuuden todellisuutta matalammalle.
- Todentamismenetelmän turvallisuudesta ja RP namesta ei muutoin kommentteja.
- Traficom yhteenveto: valmistellaan määräykseen muutoksia valmistelumuistion mukaisesti.

Muutosehdotus 6.3 Tunnistusvälineen henkilöön kytkeminen

6.3 Tunnistusvälineen henkilöön kytkeminen

Tunnistusmenetelmän todentamistekijät on kytkettävä tunnistusjärjestelmässä tunnistusvälineen haltijaan.

Tunnistusvälinettä ei saa yhdistää hakijaan ennen hakijan ensitunnistamista tai tunnistusvälineen myöntämisprosessissa on muutoin varmistettava, että tunnistusväline ei ole käytettävissä ennen kuin tunnistus- ja luottamuspalvelulain 17 §:n mukainen ensitunnistaminen on tehty.

- Ei muutoksia voimassa olevaan vaatimukseen
- Lisätään selvennys perusvaatimuksesta
  - kytkeminen on luonnollisesti erilaista eri todentamistekijöillä, esim. PIN-koodien ja biometristen tekijöiden käsittely eroaa sovelluksen tai tunnuslukulaitteen kytkemisestä

Kommentit työpajassa 10.3.2021 /tunnistusvälineen henkilöön kytkeminen

- Kysyttiin, estääkö väliaikaisen tunnistusvälineen tarjoamisen kun ensitunnistus on tehty?
  - Virasto totesi, että määräys on neutraali siihen nähden, mikä tunnistusvälineen voimassaolo on. Kysymys liittyy tilapäisvarmenteisiin ja muihin vaatimuksiin, joihin voidaan palata muussa yhteydessä.

Muutosehdotus 6.4 Tunnistusmenetelmän käyttäjäkohtaisten tietojen käsittely

6.4 Tunnistusmenetelmän käyttäjäkohtaisten tietojen käsittely

Tunnistuspalvelun ~~*Palveluntarjoajan*~~ *on varmistettava, etteivät tunnistusvälineeseen liittyvät salaiset tiedot paljastu sen henkilöstölle missään tilanteessa.*

Tunnistuspalvelun tarjoaja ~~*Palveluntarjoaja*~~ *ei saa kopioida tunnistusvälineeseen liittyviä salaisia tietoja.*

- Vrt. varmuustasoasetus
  - *2.2.1/ 2. Sähköisen tunnistamisen menetelmä on suunniteltu siten, että sitä voidaan olettaa käytettävän vain, jos se on sen henkilön hallinnassa tai hallussa, jolle se kuuluu.*
  - *2.3.1/2. Jos henkilön tunnistetiedot tallennetaan osana todentamismekanismia, nämä tiedot on suojattu niiden menetykseltä ja vaarantamiselta, mukaan lukien analyysi verkkoympäristön ulkopuolella.*
  - *2.4.6/ 3. Pääsy arkaluonteiseen salaustekniseen aineistoon, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, rajoitetaan tiukasti niihin tehtäviin ja sovelluksiin, jotka edellyttävät tällaista pääsyä. On varmistettava, ettei tällaista aineistoa koskaan tallenneta pysyväisluonteisesti ilmitekstinä. ...Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä.*
- Alustavasti vain sanamuodon tarkennus. Muita huomioita?

Kommentit työpajassa 10.3.2021 /käyttäjäkohtaisten tietojen käsittely

- Ei kommentteja

Kommentit työpajassa 10.2.2021/PSD2 -havainnot

- Ei kommentteja Traficomin koosteeseen tunnistuslain/eIDAS-sääntelyn ja PSD2 RTS SCA & CSC:n vaatimusten vertailusta.
- Fivan täydennykset EBA Q&A –poimintoihin aikaisemmalla kalvolla.

Blockchain SSI

Findyn esitys

Yleiset linjaukset määräyksen päivittämisestä

- Työsuunnitelma 7.12.2021 kohta 1.4
  - https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Määräys%2072%202020-2021%20päivittämisen%20työsuunnitelma%207.12.2020.pdf
- Blockchain ja SSI
  - julkisen ja yksityisen sektorin yhteistyön politiikkaratkaisut eivät kuulu valvontaviranomaisen toimivaltaan tai tehtäviin
  - Määräystyön yhteydessä varataan tilaisuus käsitellä lohkoketjuteknologian ja SSI -lompakkototeutusten suhdetta tunnistuksen teknisiin vaatimuksiin ja arviointivaatimuksiin
  - virasto ei ole tässä vaiheessa tekemässä omaa teknistä yksityiskohtaista arviota, mutta seuraa tarkasti eIDAS-asetuksen uudelleenarviointia ja EU-tason hankkeita

Kommentit työpajassa 10.3.2021/ SSI, Blockchain vrt. tunnistuspalvelun vaatimukset

- Findyn esittämät kalvot julkaistaan erikseen
- Ei vaikutuksia määräykseen tässä vaiheessa

Seuraava työpaja

- 5/7 Luottamuspalvelut: palveluiden ja arvioinnin ETSI-standardit
  - Ke 15.4.2021
  - Muistio tulee arviolta 1.4.2021
  - Huom. Mahdollinen jatkotyöpaja ennakkosuunnitelmasta poiketen TO 22.4.2021 klo 9-11
- Työpaja 6/7 KE 12.5.2021
  - Tunnistusvaatimusten muutosehdotukset, joita on työstetty eteenpäin aihekohtaisten työpajojen jälkeen ja linjattu virastossa
  - Materiaali 3.5.
- Työpaja 7/7 KE 10.6.
  - Kokonaisuus, ”saatekeskustelu” ennen viimeistelyä, käännöksiä ja lausuntokierrosta

Kommentit 10.3.2021 /seuraavat työpajat, valmisteluprosessi

- Ei kommentteja
- Traficom muistutti, että kahdenvälisiä tapaamisia voi pyytää, jos on tarpeen käsitellä asioita, joita ei voi tuoda esille avoimissa työpajoissa.

Kiitos osallistumisesta, olkaa yhteydessä

eidas@traficom.fi

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus