VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Tiedonhallintalautakunta
Informationshanteringsnämnden

Suositus teknisistä rajapinnoista ja katseluyhteyksistä

Lautakunnat

Valtiovarainministeriön julkaisuja – 2021:21

Valtiovarainministeriön julkaisuja 2021:21

Suositus teknisistä rajapinnoista ja katseluyhteyksistä

Valtiovarainministeriö Helsinki 2021

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Julkaisumyynti
Beställningar av publikationer

Valtioneuvoston verkkokirjakauppa

Statsrådets
nätbokhandel

vnjulkaisumyynti.fi

Valtiovarainministeriö

ISBN pdf: 978-952-367-489-9
ISSN pdf: 1797-9714

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2021

Kuvailulehti
3.5.2021

Suositus teknisistä rajapinnoista ja katseluyhteyksistä

Valtiovarainministeriön julkaisuja 2021:21		**Teema**	Lautakunnat
Julkaisija	Valtiovarainministeriö		
Yhteisötekijä	Tiedonhallintalautakunta		
Kieli	Suomi	**Sivumäärä**	20

Tiivistelmä

Julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019, jatkossa tiedonhallintalaki) säädetään teknisten rajapintojen ja katseluyhteyksien kautta tapahtuvien tietojen luovutusten toteutustavoista. Teknisellä rajapinnalla tarkoitetaan sähköisen tiedonvaihdon mahdollistavaa tiedonsiirtoratkaisua kahden tai useamman tietojärjestelmän välillä.

Tämä suositus sisältää tarkennuksia tiedonhallintalaissa säädettyjen sähköisten luovutustapojen toteuttamiseen. Suositus ei ole sitova, vaan siinä esitetään, miten viranomaiset voivat toteuttaa sähköiset luovutukset tiedonhallintalain edellyttämällä tavalla.

Tiedonhallintalautakunta hyväksyi suosituksen 31.8.2020.

Asiasanat	tiedonhallintalautakunta, tiedonhallintalaki, katseluyhteys, lautakunnat, suositukset, rajapinnat (tietokoneohjelmat), sähköinen hallinto, viranomaiset		
ISBN PDF	978-952-367-489-9	**ISSN PDF**	1797-9714
Julkaisun osoite	http://urn.fi/URN:ISBN:978-952-367-489-9		

Presentationsblad
3.5.2021

Rekommendation om tekniska gränssnitt och elektroniska förbindelser

Finansministeriets publikationer 202121		**Tema**	Nämnder
Utgivare	Finansministeriet		
Utarbetad av	Informationshanteringsnämnden		
Språk	Finska	**Sidantal**	20

Referat

I lagen om informationshantering inom den offentliga förvaltningen (906/2019, nedan informationshanteringslagen) finns bestämmelser om hur informationsöverföringen via tekniska gränssnitt och elektroniska förbindelser ska ske. Med tekniskt gränssnitt avses en kommunikationsmetod för elektroniskt informationsutbyte mellan två eller flera informationssystem.

Denna rekommendation innehåller preciseringar som gäller elektronisk överföring enligt informationshanteringslagen. Rekommendationen är inte bindande, utan redogör för hur myndigheterna kan genomföra elektronisk överföring på det sätt som krävs enligt informationshanteringslagen.

Informationshanteringsnämnden godkände rekommendationen den 31 augusti 2020..

Nyckelord informationshanteringsnämnden, informationshanteringslagen, elektronisk förbindelse, nämnder, rekommendationer, gränssnitt, e-förvaltning, myndigheter

ISBN PDF	978-952-367-489-9	**ISSN PDF**	1797-9714
URN-adress	http://urn.fi/URN:ISBN:978-952-367-489-9		

Description sheet
3 May 2021

Recommendation concerning technical interfaces and viewing access

Publications of the Ministry of Finance 2021:21		**Subject**	Board
Publisher	Ministry of Finance		
Group Author	Information Management Board		
Language	Finnish	**Pages**	20

Abstract

The Act on Information Management in Public Administration (906/2019), also known as the Information Management Act, includes provisions on methods of disclosing information via technical interfaces and viewing access arrangements. A technical interface means a data transfer solution enabling electronic data transfer between two or more information systems.

This recommendation sets out further details concerning implementation of the electronic disclosure methods referred to in the Information Management Act. The recommendation is not binding but sets out how public authorities can implement electronic disclosure in the manner required by the Information Management Act.

This recommendation was approved by the Information Management Board on 31 August 2020.

Keywords Information Management Board, Information Management Act, viewing access, boards, recommendations, interfaces (computer programs), e-government, public authorities

ISBN PDF	978-952-367-489-9	**ISSN PDF**	1797-9714
URN address	http://urn.fi/URN:ISBN: 978-952-367-489-9		

Sisältö

1 Johdanto

Julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019, jatkossa tiedonhallintalaki) säädetään teknisten rajapintojen ja katseluyhteyksien kautta tapahtuvien tietojen luovutusten toteutustavoista. Teknisellä rajapinnalla tarkoitetaan sähköisen tiedonvaihdon mahdollistavaa tiedonsiirtoratkaisua kahden tai useamman tietojärjestelmän välillä. Tiedonhallintalain säännökset eivät ole tiedonsaantiin oikeuttavia, vaan niissä on säädetty sähköisen luovutustavan toteuttamisesta ja ehdoista niissä tilanteissa, joissa sähköinen luovuttaminen tapahtuu teknisten rajapintojen tai katseluyhteyksien avulla. Tekniset rajapinnat ja katseluyhteydet voivat toiminnoiltaan olla jossain määrin päällekkäisiä, eikä aina ole tarkoituksenmukaista toteuttaa molempia samaan käyttötarkoitukseen.

Teknisiä rajapintoja ja katseluyhteyksiä käytettäessä on huolehdittava siitä, että luovutettavat tiedot ovat käyttötarkoitukseensa nähden ajantasaisia. Tiedonhallintalain 20.1 §:n mukaan viranomaisen on pyrittävä hyödyntämään toisen viranomaisen tietoaineistoja, jos viranomaisella on oikeus saada tarvittavat tiedot toiselta viranomaiselta teknisen rajapinnan tai katseluyhteyden avulla. Tietojen hyödyntämisessä on huolehdittava asianosaisen tai muun hallinnon asiakkaan oikeusturvasta.

Tämä suositus sisältää tarkennuksia tiedonhallintalaissa säädettyjen sähköisten luovutustapojen toteuttamiseen. **Suositus ei ole sitova, vaan siinä esitetään, miten viranomaiset voivat toteuttaa sähköiset luovutukset tiedonhallintalain edellyttämällä tavalla.**

Teknisiä rajapintoja ja katseluyhteyksiä koskeva sääntely korvaa aiemmin säädetyt teknisiä käyttöyhteyksiä koskevat säännökset. Tiedonhallintalautakunta pitää tarpeellisena, että siirtymäaikana arvioidaan, onko aiemmin toteutetut sähköiseen tietojensiirtoon liittyvät menettelyt olleet tosiasiassa teknisiä käyttöyhteyksiä. Esimerkiksi tietojen toimittaminen viranomaiselle käyttämällä digitaalisessa palvelussa olevaa lomaketta ei ole teknisen rajapinnan tai katseluyhteyden avulla tapahtuvaan tietojen luovuttamista, vaan tietojen toimittamista vastaanottavalle viranomaisen sähköistä tiedonsiirtomenetelmää käyttämällä. Sähköisiä tiedonsiirtomenetelmiä koskevaa sääntelyä on sähköisestä asioinnista viranomaistoiminnassa annetussa laissa (13/2003) sekä digitaalisten palvelujen tarjoamisesta annetussa laissa (306/2019).

2 Teknisten rajapintojen kautta tapahtuva tietojen luovuttaminen

Teknisen rajapinnan käyttöä koskevia säännöksiä sovelletaan tilanteissa, joissa tiedonvaihto tapahtuu automaattisesti tietojärjestelmien välillä. Mainittuja säännöksiä ei sovelleta, jos tietoja tallennetaan tietojärjestelmään esimerkiksi käyttäjän käyttäessä jotain sähköistä lomaketta tai digitaalista palvelua. Tällöin tietojen tallentaminen tai siirtäminen tapahtuu sähköistä tiedonsiirtomenetelmää käyttämällä.

2.1 Tietojen luovuttaminen tietojärjestelmien välillä

Tiedonhallintalain 22.1 §:n mukaan viranomaisten on toteutettava säännöllisesti toistuva ja vakiosisältöinen sähköinen tietojen luovuttaminen tietojärjestelmien välillä teknisten rajapintojen avulla, jos vastaanottavalla viranomaisella on tietoihin laissa säädetty tiedonsaantioikeus. Kun viranomaisten välillä tapahtuu säännöllisesti toistuvaa tietojen luovuttamista sähköisessä muodossa, on luovuttaminen toteutettava teknisten rajapintojen avulla. Tiedonhallintalaissa ei ole säädetty säännöllisyydestä sen tarkemmin, joten säännöllisesti toistuva tietojen luovuttaminen voi tapahtua esimerkiksi päivittäin, viikoittain, kerran toimikaudessa tai jopa kerran vuodessa.

Teknisten rajapintojen avulla tapahtuva tietojen luovuttaminen on velvoitettua, jos tietojen luovuttaminen on vakiosisältöistä, esimerkiksi jos välitettävän tiedon rakenne ei merkittävästi muutu luovutusten välillä. Tietojen luovuttamista ei voida toteuttaa teknisiä rajapintoja hyödyntämällä, jos tietojen luovuttamiseen liittyy luovuttavalle viranomaiselle harkintamahdollisuus siihen, mitkä tiedot ovat välttämättömiä viranomaisen tiedonsaantioikeuden ja tiedon käyttötarpeen näkökulmasta. Silloin, kun tiedot saavan viranomaisen tiedonsaantioikeus rajautuu vain välttämättömiin tietoihin, on erikseen selvitettävä, liittyykö tietojen antamiseen tapauskohtaista harkintaa, jolloin luovutettava tietosisältökään ei ole vakiomuotoista. Siten mitä tahansa tietoa ei voida luovuttaa tietojärjestelmien välillä teknisten rajapintojen avulla automaattisesti.

Teknisten rajapintojen rakenteet määrittelee luovuttava viranomainen, jolla on myös toimivalta päättää tietojen luovuttamisesta. Tiedot luovuttava viranomainen määrittelee siten käytännössä ne tilanteet, joissa rajapinta voidaan avata toiselle viranomaiselle ottaen

huomioon, mitä laissa on säädetty tietojen luovuttamismahdollisuudesta ja velvollisuudesta tietojen luovuttamiseen.

Tietoja voidaan luovuttaa viranomaisten tietojärjestelmien välillä teknisten rajapintoja avulla myös tilanteissa, joissa tietojen luovuttaminen ei ole säännöllistä, jos luovutettavat tiedot ovat vakiosisältöisiä. Kuitenkin tällöin yksittäisten tietoluovutusten toteuttamiseen voi löytyä taloudellisesti ja teknisesti tarkoituksenmukaisempia keinoja. Näissä tilanteissa tietojen luovuttaminen voi olla tehokkaampaa käyttämällä jotain digitaalista palvelua, kuten turvasähköpostia tai muuta sähköistä tiedonsiirtomenetelmää.

Tietojen luovuttamisesta päättää se **viranomainen**, jonka asiakirjoihin tai tietoihin teknisen rajapinta avataan, ei tietojärjestelmän teknisestä ylläpidosta vastaava toimija, kuten **palvelukeskus**. Päätettäessä teknisen rajapinnan avaamisesta tietoja luovuttava viranomainen ei voi asettaa tietojen luovuttamiselle sellaisia ehtoja, joista on säädetty tiedonhallintalaissa tai muussa laissa, eivätkä ehdot voi olla ristiriidassa laissa säädetyn kanssa. Tiedot luovuttava viranomainen voi asettaa tietoluovutuksille ehtoja siltä osin kuin ne tarkentavat tiedonhallintalain 4 luvussa olevia tietoturvallisuusvaatimuksia. Ehtojen laadinnassa on suositeltavaa hyödyntää tiedonhallintalautakunnan antamia tietoturvallisuussuosituksia. Teknisen rajapinnan avaamista koskevasta päätöksestä on ilmettävä mihin käyttötarkoitukseen tietoja luovutetaan ja minkä laissa säädetyn tiedonsaantioikeuden perusteella tietojen luovuttaminen tapahtuu.

2.2 Poikkeukset tietojen luovuttamisessa tietojärjestelmien välillä

Tiedonhallintalaissa säädetty velvollisuus teknisten rajapintojen käyttöön sisältää joitakin poikkeuksia. Säännöllisesti toistuva ja vakiosisältöinen tietojen luovuttaminen voidaan toteuttaa ilman teknisten rajapintojen käyttöä, jos sellaisen toteuttaminen tai käyttö ei ole teknisesti tai taloudellisesti tarkoituksenmukaista. Poikkeus voi tulla kysymykseen tilanteissa, joissa käytettävät tietojärjestelmät ovat elinkaarensa loppuvaiheessa, jolloin rajapintojen toteuttamisen vanhaan tietojärjestelmään ei ole teknisistä tai taloudellisista syistä tarkoituksenmukaista. Viranomaisen on kuitenkin näissä tilanteissa arvioitava perusteet sille, miksi tietojen luovuttamista ei voida toteuttaa tiedonhallintalaissa säädetyn velvoitteen mukaisesti. Arviointi on sisällytettävä osaksi tiedonhallintalain 5 §:ssä säädettyä tiedonhallinnan muutosvaikutusarviointia, jos teknistä rajapintaa ei toteuteta tiedonhallintaan liittyvän muutoksen tai uuden tietojärjestelmän käyttöönoton yhteydessä.

2.3 Edellytykset tietojen luovuttamiselle tietojärjestelmien välillä

Tietoja luovuttavan viranomaisen tulee selvittää vastaanottavan viranomaisen tiedonsaantioikeudet, vakiosisältöisesti luovutettavat tiedot sekä säännöllisen tietojen luovuttamisen ajallinen toistettavuus. Selvityksen perusteella tietoja luovuttava viranomainen määrittelee vastaanottajakohtaisesti rajapinnan tietorakenteet, mikäli eri viranomaisten tiedonsaanti poikkeaa toisistaan. Jos tietojen luovuttaminen edellyttää tapauskohtaista arviointia sekä luovutettavat tiedot poikkeavat tapauskohtaisesti, ei tietojen luovuttaminen ole suositeltavaa teknisten rajapintojen avulla, koska tällaista harkintaa ei voida automatisoida. Sen sijaan, jos käyttötarve vaihtelee eri tehtävien perusteella ja näissä tietosisältö on vakiosisältöistä, voi luovutettavien tietojen laajuus ja määrä vaihdella samaakin teknistä rajapintaa käytettäessä.

Käyttöoikeudet määritellään tiedot pyytävään järjestelmään. Käyttöoikeusmäärittely luovuttavaan tietojärjestelmään tarkoittaa lähinnä tiedot saavan tietojärjestelmän käyttöoikeuden määrittelyä. Käyttöoikeuksien lisäksi määritellään tiedot saavan tietojärjestelmän tunnistamisessa tarvittavat tiedot. Käyttöoikeuksien määrittelyyn vaikuttavat tietojärjestelmän käyttäjän työtehtävät sekä luovutettavien tietojen tiedonsaantiperuste ja käyttötarkoitus. Tiedot luovuttava viranomainen voi asettaa erityisiä, mutta lakiin perustuvia ehtoja tiedot saavan viranomaisen tietojärjestelmän käyttöoikeuksille. Käyttöoikeuksien myöntämisessä tulee noudattaa tiedonhallintalain 16 §:ssä kuvattuja vaatimuksia.

Salassa pidettävien tietojen tai henkilötietojen luovuttamisen tarpeen tai välttämättömyyden tapauskohtainen varmistaminen voidaan toteuttaa esimerkiksi siten, että haettaessa toisen tietojärjestelmän sisältämiä tietoja rajapinnan avulla reaaliaikaisesti, kontrolloi tiedot pyytävä tietojärjestelmä käyttäjän toimintaa. Kontrolleina on suositeltavaa käyttää seuraavia:

- Tiedot pyytävä tietojärjestelmä informoi käyttäjää siitä, mihin tarkoitukseen tietoja voidaan käyttää ja
- pyytää käyttäjää yksilöimään ennalta määritellyistä käyttötarkoituksista sen, johon tietoja pyydetään luovuttamaan, jos tietoja voidaan käyttää useisiin käyttötarkoituksiin.
- Prosessiohjatuissa tietojärjestelmissä käyttötarpeen selvittäminen ei ole tarpeen, koska rajapinta on avattu toiseen tietojärjestelmään vain tiettyä yksittäistä käyttötarkoitusta varten, jolloin käyttötarkoitus ilmoitetaan osana käyttäjälle annettavaa informointia.
- Tietojen saantia koskeva peruste sisällytetään osaksi sekä tiedot luovuttavan että tiedot vastaanottavan tietojärjestelmän luovutuslokitietoja.

Jos tietojen luovuttaminen tapahtuu viranomaisten tietojärjestelmien välillä automaattisesti säännöllisin väliajoin, kuten eräajopohjaisissa tai muissa tiedostopohjaisissa tietoluovutuksissa, lain vaatimukset voidaan täyttää esimerkiksi rekisteröimällä luovutuslokiin tiedot siitä, mitä tietoja ja mihin käyttötarkoitukseen ne on luovutettu. Näissä tilanteissa luovutuksen teknisessä toteutuksessa on kiinnitettävä huomiota siihen, että luovutettavat tiedot ovat tapauskohtaisesti tarpeellisia tai välttämättömiä. Teknisin kontrollein on varmistettava, että luovutuksen saavalla viranomaisella on edelleen jatkuva tarve saada toiselta viranomaiselta asiakasta tai muuta asianosaista koskevia tietoja.

Tästä syystä teknisiä rajapintoja käytettäessä ei riitä, että tiedot toimitetaan automaattisesti luovuttavasta tietojärjestelmästä säännöllisin väliajoin. Tiedot saavan viranomaisen tietojärjestelmän on tehtävä jokaisen tietojenluovutuksen osalta tekninen tietopyyntö luovuttavalle tietojärjestelmälle, jos asiankäsittelyt perustuvat siihen, että asiakassuhde ja tiedonsaantitarve ovat määräaikaisia. Tapauskohtainen arviointi voi tapahtua myös siten, että tiedot luovuttava tietojärjestelmä tunnistaa asiakkaiden tiedoissa olevat muutokset ja välittää ne edelleen automaattisesti tiedot vastaanottaviin järjestelmiin, jos tietojen luovuttaminen perustuu jatkuvaan tietotarpeeseen esimerkiksi eräajopohjaisissa tietoaineistopäivityksissä.

2.4 Yhteentoimivuus ja tietojen siirron toteuttaminen

Yhteentoimivuuteen liittyvät vaatimukset teknisten rajapintojen osalta edellyttävät yhteentoimivuuden huomioimista ja varmistamista niin teknisen toteutuksen (rajapinta ja tiedonsiirtoyhteys), semanttisen toteutuksen (sanastot ja koodistot) kuin tietomallinnuksen (metatiedot ja rakenteisuus) osalta. Käytettävien sanastojen tulisi perustua laissa säädettyihin käsitteisiin eikä niitä tulisi määritellä uudelleen toiseen merkitykseen tai toisen sisältöisenä. Sanastojen määrittelyyn vaikuttaa se, että perustuslain 2.3 §:n mukaan kaikessa julkisessa toiminnassa on tarkoin lakia noudatettava. Laissa säädetyt käsitteet sitovat niiden käyttöä viranomaisten toiminnassa. Yhteentoimivuuden edistämiseksi suositellaan, että kuvaamisessa käytetään yhteisiä sanastoja, tietomalleja ja koodistoja.

Hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetussa laissa (571/2016, tukipalvelulaki) säädetään tiedonvälityskanavasta eli palveluväylästä, jonka avulla käyttäjäorganisaatiot voivat siirtää ja luovuttaa tietovarantoihinsa sisältyviä tietoja ja tarjota asiointipalveluja. Tukipalvelulain 5.1 §:n mukaan valtion hallintoviranomaiset, virastot, laitokset ja liikelaitokset, kunnalliset viranomaiset niiden hoitaessa laissa niille säädettyjä tehtäviä sekä tuomioistuimet ja muut lainkäyttöelimet ovat velvollisia käyttämään palveluväylää, kun se on käytettävissä ja palveluväylää vastaavan itsenäisesti hankitun palvelun palvelusopimus on päättynyt, jollei viranomaisen ole teknisistä, toiminnallisista tai

kustannustehokkuuteen tai tietoturvallisuuteen liittyvistä syistä välttämätöntä käyttää toiminnassaan tai sen osassa muuta palvelua.

Jokainen palveluväylään liittynyt organisaatio hallitsee omien järjestelmiensä tietoja ja vastaa siitä, että muiden tarvitsemat tiedot ovat saatavissa ja kuvattuna väylän liitynnät esittävään katalogiin (liityntäkatalogi). Lisäksi organisaation on itse huomioitava tietojen jakoon liittyvät mahdolliset rajoitukset.

Valtion, kuntien ja kuntayhtymien tiedonhallintayksikköjen tulee käyttää tietojen siirtoon teknisten rajapintojen avulla palveluväylää, ellei palveluväylän käyttämättä jättämiseen ole laissa säädetyn perusteella poikkeamisperustetta esimerkiksi tiedostosirtotyyppisten ratkaisujen käyttöön. Tällaiset poikkeamisperusteet tulisi kirjata tiedonhallinnan muutosvaikutusarviointiin, joka on tehtävä tiedonhallintalain 5.3 §:n nojalla silloin, kun tiedonhallinnan muutos johtaa olennaisiin muutoksiin tiedonhallintayksikön tiedonhallintamallissa.

3 Katseluyhteys

3.1 Katseluyhteyden avaamisen edellytykset

Viranomainen voi avata katseluyhteyden toiselle viranomaiselle tietovarannon sellaisiin tietoihin, joihin katseluoikeuden saavalla viranomaisella on tiedonsaantioikeus.

Tietoja luovuttavan viranomaisen tulee käydä tiedonsaantioikeudet läpi vastaanottavan viranomaisen kanssa. Tiedonsaantioikeuksien perusteella määritellään katseluyhteyden näkymä, joka perustuu kunkin viranomaisen tiedonsaantioikeuksiin ja voi siten olla eri viranomaisille erilainen.

Katseluyhteyden käyttöoikeudet myönnetään vastaanottavalle viranomaiselle tiedonsaantioikeuksien ja -tarpeen perusteella. Viranomainen, jolle käyttöoikeudet myönnetään, vastaa siitä, ettei käyttöoikeuksia ja niihin liittyviä tunnuksia liittyvä tunnuksia tai niiden avulla hankittuja tietoja luovuteta oikeudettomille henkilöille ja että käyttöoikeuksia käytetään vain siihen tarkoitukseen, johon ne on myönnetty.

Lisäksi viranomaisen tulee ilmoittaa käyttäjien virkoihin liittyvistä muutoksista käyttöoikeudet myöntäneelle viranomaiselle siltä osin, kuin ne vaikuttavat käyttöoikeuksien hallintaan, kuten oikeuksien muuttamiseen, jäädyttämiseen tai poistamiseen. Käyttöoikeudet myöntäneen viranomaisen vastuulla on varmistaa käyttöoikeuksien ajantasaisuus ja käyttöoikeuksien mukaisen pääsyn toteutuminen.

Käyttöoikeuksien myöntämisessä tulee noudattaa tiedonhallintalain 16 §:ssä kuvattuja vaatimuksia.

3.2 Katseluyhteyden toteuttaminen

Katseluyhteyttä tarjoavan viranomaisen tulee toteuttaa järjestelmä siten, että se tukee katselumahdollisuuden rajaamista vain tiedonsaantioikeuden määrittämiin tarpeellisiin tai välttämättömiin tietoihin.

Katseluyhteyttä tarjoava viranomainen voi toteuttaa tämän arvioimalla ja dokumentoimalla katselumahdollisuuden saavan viranomaisen tehtävien hoitamisen kannalta tarpeelliset tai välttämättömät tiedot. Katseluyhteyttä tarjoava viranomainen voi toteuttaa

järjestelmän teknisesti siten, että katselumahdollisuus rajataan tietotarpeen tai välttämättömien tietojen perusteella viranomais- tai käyttäjäkohtaisesti.

Katseluyhteyttä tarjoavan viranomaisen tulee toteuttaa katseluyhteys siten, että tietoja voidaan hakea ainoastaan yksittäisinä hakuina. Tällöin hakukriteerien on oltava sellaisia, että niiden perusteella ei voida hakea suurta määrää useita henkilöitä koskevia tietoja, vaan haku rajautuu pääsääntöisesti yhden tai muutamaan kriteerit täyttävän henkilön tietoihin.

Vaatimusta voidaan myös edesauttaa toteuttamalla katseluyhteys tietoteknisesti esimerkiksi siten, että tietoja haettaessa käyttäjä syöttää tai valitsee esimerkiksi valikosta tietojen hakemisen perusteen. Peruste käyttäjätietoineen jää katseluyhteyden avulla kerättäviin luovutuslokitietoihin, jolloin jälkikäteen voidaan todentaa kunkin katseluyhteyden avulla tehdyn haun käyttötarkoitus ja lainmukainen oikeusperuste käsittelylle. Tämä menettely pakottaa käyttäjän arvioimaan kullakin hakukerralla ennen haun tekemistä, onko haku tarpeellinen virka- tai työtehtävien hoitamisen kannalta. Tällä pyritään osaltaan estämään myös se, ettei hakuja voida tehdä automaattisesti esimerkiksi hakurobotin avulla.

Katseluyhteyttä tarjoavan viranomaisen tulee toteuttaa katseluyhteys tietovarantoon niin, että katseluyhteyden mahdollistava tietojärjestelmä tunnistaa automaattisesti poikkeavat tietohaut. Lisäksi on suositeltavaa, että tietojärjestelmä pyrkii estämään tietohakujen jatkumisen, kunnes poikkeama on selvitetty. Lisäksi tulisi olla ennalta määritelty prosessi, jossa pystytään selvittämään nopeasti poikkeuksellisten tietohakujen syyt. Tällaiset poikkeamat on suositeltavaa ohjata esimerkiksi järjestelmän pääkäyttäjälle tai tietosuojavastaavalle jatkoselvittelyjä varten. Tiedot saavan viranomaisen työnantaja-asemassa olevien virkamiesten tulisi selvittää tietojen hakijan tekemien hakujen perusteet sekä antaa tästä selvitys tiedot luovuttavalle viranomaiselle.

Poikkeavilla tietohauilla tarkoitetaan esimerkiksi seuraavaa:

1. Käyttäjä hakee sellaisia tietoja, joihin hänellä ei oletetusti ole oikeutta tai hän tekee lyhyen ajan sisään poikkeuksellisen paljon hakuja. Riskiä voidaan hallita laatimalla erilaisia hälyttimiä poikkeavan käytön tunnistamiseksi. Hälytin tekee varoituksen esimerkiksi tilanteissa, joissa haut selvästi kohdistuvat käyttäjän tehtävien ulkopuolelle tietosisällön tai maantieteellisen sijainnin osalta, tai haut tapahtuvat tavallisesta poikkeavaan ajankohtaan.
2. Jotain yksittäistä tietoa tai jonkin yksittäisen henkilön tietoja haetaan tavallista enemmän.
3. Käyttäjä syöttää hakukenttään tavanomaisesta poikkeavia hakusanoja tai erikoismerkkejä, tai käyttäjän toiminta viittaa selvästi tavallisesta poikkeavaan toimintaan, jonka tarkoituksena on murtaa järjestelmän suojaukset. Tätä riskiä

voidaan hallita suorittamalla järjestelmälle ennen käyttöönottoa asianmukainen tietoturvatestaus, jossa huomioidaan esimerkiksi tietokantahyökkäyksiltä suojautumisen tarpeet. Lisäksi tulee estää sellaisten hakusanojen tai -merkkien syöttäminen, joita ei oletetusti tarvitse käyttää.

Mikäli jokin asetetuista hälyttimistä hälyttää, niin järjestelmä voi esimerkiksi ilmoittaa tästä käyttäjälle, sulkea käyttäjän käyttöoikeudet, päättää käyttäjän katseluyhteyden ja kertoa mihin voi olla yhteydessä käyttäjätunnusten aktivoimiseksi uudelleen. Lisäksi hälytystapahtuman tulee toimia käynnistimenä tätä varten suunnitellulle tietoturvapoikkeaman selvitysprosessille.

Poikkeavien tietohakujen automaattinen tunnistus voidaan toteuttaa usealla tavalla ja teknologialla. Toteuttamiseen löytyy niin avoimeen lähdekoodiin perustuvia kuin kaupallisia ratkaisuja. Yksinkertaisimmillaan toteutuksessa voidaan käyttää järjestelmää, jonka toiminnallisuudet mahdollistavat poikkeavan toiminnan havaitsemisen ja siitä hälyttämisen esimerkiksi lokien analysointiin asetettujen sääntöjen perusteella. Sääntöpohjaiset järjestelmät tunnistavat kuitenkin vain **ennalta määritellyt** poikkeavat toiminnat. Siten ne edellyttävät sääntöjen toimivuuden jatkuvaa arviointia ja kehittämistä. Poikkeavan toiminnan tunnistamista voidaan edelleen parantaa esim. hyödyntämällä koneoppimista tai muuta edistynyttä analytiikkaa sääntöjä täydentämässä.

4 Yleisten tietoturvallisuustoimenpide-vaatimusten soveltaminen teknisiin rajapintoihin ja katseluyhteyksiin

4.1 Riskiperusteinen suunnittelu

Viranomaisen tulee arvioida teknisten rajapintojen ja katseluyhteyksien toteuttamiseen liittyvät riskit sekä suunnitella toimenpiteet riskien hallitsemiseksi siten, että sähköiset tiedonsiirtomenetelmät voidaan toteuttaa ja niitä voidaan käyttää turvallisella tavalla. Riskien arvioinnissa ja hallitsemisessa tulee huomioida tiedonhallintalain 4 luvussa määritellyt tietoturvallisuuden vähimmäisvaatimukset. Perusrekistereitä ylläpitävien, terveystietoja välittävien sekä muiden teknisten rajapintojen kautta tavallista enemmän tietoa luovuttavien viranomaisten on hyvä laatia kattava riskienarviointi. Riskiarviointia suositellaan tehtäväksi tietoja luovuttavien ja vastaanottavien toimijoiden yhteistyönä, sekä toisaalta yhdessä muiden samoja tai samankaltaisia tehtäviä hoitavien viranomaisten kanssa. Näin mahdollistetaan riskien ja hyvien käytänteiden jakaminen toimijoiden kesken.

Teknisten rajapintojen ja katseluyhteyksien toteuttamiseen ja käyttämiseen liittyvässä riskienarvioinnissa tunnistetaan olennaiset riskit, jotka voivat vaikuttaa kyseisten rajapintojen ja katseluyhteyksien käytettävyyteen ja saatavuuteen tai niissä käsiteltävien tietoaineistojen tietoturvallisuuteen. Riskejä voivat aiheuttaa esimerkiksi hyökkäysmenetelmiltä suojautumiseen, avaintenhallintaan, lähetettävän tiedon laatuun tai tiedonsiirron automaatioon liittyvät puutteet tai muut tiedonsiirtomenetelmien turvallisuusongelmat.

Lisäksi riskejä voi aiheuttaa puutteet vastaanottavan viranomaisen tietojenkäsittely-ympäristössä, osaamattomuus sähköisten tiedonsiirtomenetelmien tai lähdejärjestelmän käyttämisessä tai vastaanotettavien tietojen käsittelyssä.

Näitä riskejä voidaan pyrkiä hallitsemaan varmistamalla tietoja vastaanottavien viranomaisten ja järjestelmien käyttäjien tietoturvaosaaminen liittyen kyseisen järjestelmän erityispiirteisiin ja käsiteltäviin tietoihin. Siten tietoja luovuttavan viranomaisen tulee ohjeistaa ja tarvittaessa varmistaa osaaminen esimerkiksi kouluttamalla:

- Miten sähköistä tiedonsiirtomenetelmää ja tietojärjestelmää tulee käyttää, jotta käyttäjä kykenee välttämään riskialttiita ja tietoturvallisuutta vaarantavia käyttötapoja?

- Miten järjestelmän sisältämiä tietoja tulee käsitellä, etteivät niiden luottamuksellisuus, eheys ja saatavuus vaarannu?

Tietosuojaa lisää käyttöperusteiden dokumentointi: esimerkiksi dokumentoitu tieto siitä, millä tavoin palveluun liittyvät tietopyynnöt käsitellään, kenelle ne tulee ohjata ja kuinka pitkän ajan tietoja on mahdollista pyytää ilman erillisiä kustannuksia.

Ohjeistuksen ja koulutuksen lisäksi käyttäjien huolimattomuudesta tai kiireestä aiheutuvia riskejä voidaan hallita muistuttamalla käyttäjiä ohjeista aina kirjautumisen yhteydessä.

Vastaanottavan viranomaisen tietojenkäsittely-ympäristöön liittyviä riskejä voidaan pyrkiä hallitsemaan esimerkiksi edellyttämällä tarvittavia teknisiä toimenpiteitä, selvityksiä tai kolmannen osapuolen suorittamia tietoturva-auditointeja, joilla varmistetaan tietojen käsittelyltä edellytettävät tietoturvallisuusvaatimukset.

4.2 Luovutettavien tietojen minimointi

Tietoja luovuttavan viranomaisen tulee huolehtia tietojen minimoimisesta ennen niiden luovuttamista. Tällä tarkoitetaan sitä, että viranomainen luovuttaa vain niitä tietoja, joita vastaanottava viranomainen perustellusti tarvitsee tehtävänsä hoitamiseen. Tietoja luovuttavan viranomaisen tulee varmistaa, ettei luovutettavien tietojen mukana luovuteta sellaista tietoa, jota vastaanottava viranomainen ei ole pyytänyt, jota se ei tarvitse tai johon sillä ei ole tiedonsaantioikeutta. Tämä riski saattaa koskea etenkin luovutettavissa tietoaineistossa olevia metatietoja, jotka tietoja luovuttavan viranomaisen tulisi kartoittaa ja varmistaa, ettei niissä ole sellaisia tietoja, joita ei ole syytä luovuttaa. Tietojen minimointiin kuuluu myös tarpeettomien yksilöllisten identifioivien tunnisteiden poistaminen luovutettavista tiedoista silloin, kun niiden toimittaminen ei ole erikseen perusteltua.

Jos viranomaisella on oikeus saada toisen viranomaisen tietovarannosta tehtäviensä hoitamista varten tietoja luotettavasti ja ajantasaisesti teknisen rajapinnan tai katseluyhteyden avulla, se ei saa tiedonhallintalain 20.2 §:n mukaan vaatia asiakastaan esittämään tai toimittamaan vastaavia tietoja, ellei se ole välttämätöntä asian selvittämiseksi. Luotettavuudella ja ajantasaisuudella tarkoitetaan sitä, että tiedot luovuttavalla viranomaisella tietovarannon tietoaineistojen ajantasaisuus on varmistettu ja että tietojen alkuperäisyys ja eheys on varmistettu tietoaineiston tietohuoltoon liittyvissä prosesseissa. Tietoaineiston luotettavuuteen liittyy myös se, että hallinnon asiakkaalla tulee olla mahdollisuus päästä tutustumaan näihin tietoihin sen viranomaisen tietovarannosta, josta tietoja luovutetaan toiselle viranomaiselle.

Jo suunnitteluvaiheessa on otettava huomioon mahdolliset tietojen luovuttamisen käytännöt. Järjestelmän siirroissa voi kulkea (jopa salaamattomana) tietoa, jota ei ole lupa luovuttaa joko lain perusteella tai tietosuojasäädösten vuoksi. Esimerkkinä on henkilötunnus, jota on aikaisemmin käytetty paljonkin tunnisteena järjestelmissä. Tunnistetietoja on turha siirtää datan mukana, vaikka niitä käytettäisiinkin haussa. Tällöin siirrettävä data on vain se mitä haettiin. Samoin mahdollisen tulosteen ottamisessa loppuasiakkaalle on tarkistettava, ettei tositteelle tai viranomaisen asiakirjalle turhaan tallennu asiakkaan tai pyydetyn tiedon tietosuojan alaisia muita erityissuojattavia tietoja.

4.3 Rajapintojen ja katseluyhteyksien vikasietoisuus ja käytettävyys

Lisäksi viranomaisen tulee varmistaa järjestelmään tehtävien teknisten rajapintojen ja katseluyhteyksien vikasietoisuus ja toiminnallinen käytettävyys riittävällä testauksella säännöllisesti. Vikasietoisuus tulee mitoittaa sen perusteella, kuinka kriittinen järjestelmä on toiminnan kannalta ja kuinka pitkään toimintaa voidaan jatkaa, vaikka järjestelmä ei olisi käytettävissä.

Vikasietoisuuden arvioinnissa tulee myös huomioida järjestelmien käytettävyysvaatimusten muuttuminen eri ajankohtina. Järjestelmä saattaa olla kriittinen esimerkiksi vain kuun vaihteessa tai tiettyyn aikaan vuodesta. Kriittisyyttä arvioitaessa on lisäksi huomioitava lakisääteiset tehtävät sekä riippuvuus muista järjestelmistä (oman organisaation sisällä sekä viranomaisten välillä).

Vikasietoisuuden ja toiminnallisen käytettävyyden taso tulee määritellä ennen teknisten rajapintojen ja katseluyhteyksien toteuttamista. Tekniset rajapinnat ja katseluyhteydet tulee toteuttaa määriteltyjen vaatimusten mukaisesti noudattaen turvallisen sovelluskehityksen hyviä käytäntöjä ja ohjeita. Myös teknisten rajapintojen ja katseluyhteyksien vikasietoisuus ja toiminnallinen käytettävyys tulee varmistaa säännöllisellä testauksella. Säännöllisen testauksen tuloksista on suositeltavaa ylläpitää dokumenttia, josta selviää, millaisin kriteerein vikasietoisuus ja toiminnallinen käytettävyys on varmistettu. Tämä dokumentti on suositeltavaa tiedoksi antaa niille tahoille, joiden toiminnalle rajapinta tai katseluyhteys on olennainen. Testaus tehdään vaatimusmäärittelyn mukaisesti ja testauksen säännöllisyys mitoitetaan siten, että sillä voidaan varmistaa edellytettävä vikasietoisuus ja toiminnallinen käytettävyys.

4.4 Tiedonsiirron tietoturvallisuustoimenpiteet

Viranomaisen on toteutettava teknisten rajapintojen ja katseluyhteyksien kautta tapahtuva tietojensiirto tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä. Tietojen siirtämisessä tietoverkossa on otettava huomioon tiedon eheys, luottamuksellisuus ja saatavuus. Tämän saavuttamiseksi on toteutettava riittävät tekniset ja hallinnolliset suojauskeinot. Siirrettäessä salassa pidettävää tietoa julkisen verkon kautta tietoaineisto tai tietoliikenneyhteys suojataan riittävän turvallisella salauksella kuten turvapostilla tai käyttämällä Liikenne- ja viestintäviraston hyväksymiä salausratkaisuja asiointipalvelun ja loppukäyttäjän välisen liikenteen suojaamiseen (Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksymät salausratkaisut.

Käytännön toteutustapoja turvalliselle salaukselle ovat esimerkiksi:

- käyttäjien päätelaitteiden ja viranomaisen tietojärjestelmien väliset VPN-ratkaisut,
- asiointipalvelun ja loppukäyttäjän välisen liikenteen TLS-salaus,
- organisaatioiden verkkojen välinen IPSec-salaus, sekä
- loppukäyttäjille tarjottavat turvaposti- ja tiedostosalausratkaisut.

Tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja. Käyttäjien tunnistamisessa voidaan käyttää esimerkiksi henkilökohtaisia käyttäjätunnuksia ja salasanoja. Salassa pidettäviä tietoaineistoja siirrettäessä käyttäjät tunnistetaan ja todennetaan käyttäen tunnettua ja turvallisena pidettyä tekniikkaa. Tällaisia tekniikoita ovat esimerkiksi kertakirjautuminen ja moneen tekijään perustuva todennus. Tunnistamistapa ja -vahvuus on arvioitava tapauskohtaisesti kunkin palvelun sekä siinä käsiteltävien tietojen ja niiden paljastumiseen liittyvien riskien perusteella.

Lähdejärjestelmä sekä teknisten rajapintojen ja katseluyhteyksien kautta siirrettävät tietoaineistot on suojattu teknisiltä ja fyysisiltä vahingoilta. Tämä voidaan toteuttaa esimerkiksi estämällä luvaton fyysinen pääsy tietoaineistoja käsitteleviin laitteisiin kulunhallinnan avulla. Lisäksi tiloissa, joissa siirrettäviä tietoaineistoja käsitellään, tulee huolehtia riittävistä palo-, vesi- ja sähköturvallisuuteen liittyvistä kontrolleista.

4.5 Käyttöoikeuksien hallinta ja lokitietojen kerääminen

Tietojärjestelmästä vastuussa olevan viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet myös teknisten rajapintojen ja katseluyhteyksien osalta. Käyttöoikeudet on määriteltävä käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan ja ne on pidettävä ajantasaisina.

Asianmukaisen pääsynhallinnan ja käyttäjienhallinnan avulla mahdollistetaan tietojen luvallinen käyttö ja estetään niiden luvatonta käyttöä. Ainoastaan valtuutetuille käyttäjille ja järjestelmille myönnetään pääsy- ja käyttöoikeudet ja niiden hallinnassa tulee noudattaa vähimpien oikeuksien periaatetta. Se tarkoittaa, että käyttäjille annetaan tietojärjestelmiin vain sellaiset käyttöoikeudet ja -valtuudet, jotka ovat työn suorittamiseksi välttämättömiä. Käyttäjätilien hallintaa ja käyttöä seurataan ja valvotaan poikkeamien ja uhkien havaitsemiseksi sekä niihin reagoimiseksi. Olemassa olevat käyttövaltuudet tulee arvioida säännöllisesti niiden tarpeellisuuden ja ajanmukaisuuden näkökulmasta. Käyttövaltuudet tulee näiden arviointien jälkeen päivittää vastaamaan nykytilan käyttövaltuustarpeita.

Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen. Koska teknisten rajapintojen ja katseluyhteyksien avulla luovutetaan tietoja, on näiden käytöstä kerättävä luovutuslokitiedot. Vähimmäistietoina on suositeltavaa kerätä tiedon luovutuksen tarkoitus, luovutuksen saaja (joko viranomainen tai käyttäjä), luovutettavat tietokokonaisuudet ja luovutusajankohta.

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin 0295 160 01
vm.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-367-489-9 (pdf)

Toukokuu 2021