VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Julkisen hallinnon API-periaatteet

Julkisen hallinnon ICT

Valtiovarainministeriön julkaisuja – 2022:12

Valtiovarainministeriön julkaisuja 2022:12

Julkisen hallinnon API-periaatteet

Valtiovarainministeriö Helsinki 2022

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: 978-952-367-907-8
ISSN pdf: 1797-9714

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2022

Kuvailulehti

28.2.2022

Julkisen hallinnon API-periaatteet

Valtiovarainministeriön julkaisuja 2022:12		**Teema**	Julkisen hallinnon ICT
Julkaisija	Valtiovarainministeriö		
Tekijä/t	Miina Arajärvi, Maaret Saukonoja ja Pasi Vänttinen		
Kieli	suomi	**Sivumäärä**	65

Tiivistelmä

Julkisen hallinnon API-periaatteet muodostavat yhteiset toimintaohjeet ja suositukset API-kehitykselle ja digitalisaation edistämiselle. API-periaatteet on kehitetty osana valtiovarainministeriön Tiedon hyödyntämisen ja avaamisen hanketta, joka toteuttaa pääministeri Marinin hallitusohjelman tietopolitikkaan, tiedon hyödyntämiseen ja avaamiseen liittyviä tavoitteita.

Periaatteet on jaettu kolmelle tasolle: strateginen, taktinen ja operatiivinen. Strategisen tason periaatteet ovat kohdistettu organisaation johdolle. Strategisella tasolla kuvataan, miten ohjelmointirajapintojen kehittämiselle tulisi määrittää suunta ja tavoitteet ja miten ohjelmointirajapinnat tulisi huomioida toiminnan kehittämisessä. Taktisen tason periaatteet ovat kohdistettu organisaation tiedonhallintaa kehittäville toimijoille. Taktisen tason periaatteet ohjaavat, miten ohjelmointirajapintojen kehittämistä ja ohjelmointirajapintojen muodostamaa kokonaisuutta tulisi hallita. Operatiivisen tason periaatteet ovat kohdistettu ohjelmointirajapintoja kehittäville ja ylläpitäville toimijoille. Operatiivisen tason periaatteet ohjaavat, miten yksittäisiä ohjelmointirajapintoja tulisi kehittää ja ylläpitää.

Asiasanat julkisen hallinnon ICT, API (Application Programming Interface), rajapinta, ohjelmointirajapinta, tieto, tietojärjestelmä, yhteentoimivuus, tiedonhallinta, tietopolitiikka

ISBN PDF	978-952-367-907-8	**ISSN PDF**	1797-9714
Hankenumero	VN/5386/2020		
Julkaisun osoite	https://urn.fi/URN:ISBN:978-952-367-907-8		

Presentationsblad

28.2.2022

API-principer för den offentliga förvaltningen

Finansministeriets publikationer 2022:12		**Tema**	Offentliga förvaltningens ICT
Utgivare	Finansministeriet		
Författare	Miina Arajärvi, Maaret Saukonoja och Pasi Vänttinen		
Språk	finska	**Sidantal**	65

Referat

API-principerna för den offentliga förvaltningen bildar gemensamma instruktioner och rekommendationer för API-utveckling och främjandet av digitalisering. API-principerna har utvecklats som en del av finansministeriets projekt Utnyttja och öppna information genomför mål, som genomför informationspolitik och utnyttjandet och öppnandet av information i statsminister Marins regeringsprogram.

Principerna är indelade i tre nivåer: strategisk, taktisk och operativ. Principerna på strategisk nivå är riktade till organisationens ledning. På den strategiska nivån beskrivs hur organisationen ska bestämma riktningen och målen för utvecklingen av applikationsprogrammeringsgränssnitten och hur applikationsprogrammeringsgränssnitten ska beaktas vid utvecklingen av verksamheten. Principerna på taktisk nivå är riktade till de aktörer som utvecklar informationshanteringen i organisationen. Principerna på taktisk nivå styr hur utvecklandet och helheten av applikationsprogrammeringsgränssnitt ska hanteras. Principerna på operativ nivå är riktade till de aktörer som utvecklar och administrerar applikationsprogrammeringsgränssnitt. Principerna på operativ nivå styr hur enskilda applikationsprogrammeringsgränssnitt ska utvecklas och administreras.

Nyckelord offentliga förvaltningens ICT, API (Application Programming Interface), gränssnitt, applikationsprogrammeringsgränssnitt, information, informationssystem, interoperabilitet, informationshantering, informationspolitik

ISBN PDF	978-952-367-907-8	**ISSN PDF**	1797-9714
Projektnummer	VN/5386/2020		
URN-adress	https://urn.fi/URN:ISBN:978-952-367-907-8		

Description sheet

28 February 2022

Public Administration API Principles

Publications of the Ministry of Finance 2022:12		**Subject**	Public Sector ICT
Publisher	Ministry of Finance		
Author(s)	Miina Arajärvi, Maaret Saukonoja and Pasi Vänttinen		
Language	Finnish	**Pages**	65

Abstract

The Public Administration API Principles provide common instructions and recommendations for API development and the promotion of digitalisation. The API principles have been developed under the Ministry of Finance's project on opening up and using public data, which implements the objectives related to information policy and the opening and use of public data in the Programme of Prime Minister Marin's Government.

These principles have been divided into three levels: strategic, tactical and operative. Strategic principles apply to the organisation's management. These principles describe how the direction and goals of API development should be defined and how APIs should be taken into account in the development of operations. Tactical principles apply to the developers of information management in the organisation. They guide the management of API development and the organisation's system of APIs. Operative principles apply to those who develop and maintain APIs. They guide the development and maintenance of individual APIs.

Keywords public sector ICT, API (Application Programming Interface), Interface, Data, Information System, Interoperability, Data Management, Information Policy

ISBN PDF	978-952-367-907-8	**ISSN PDF**	1797-9714
Project number	VN/5386/2020		
URN address	https://urn.fi/URN:ISBN:978-952-367-907-8		

Sisältö

1 Johdanto

Pääministeri Marinin hallitusohjelmassa[1] syvennetään tietopolitiikan johtamista ja julkisen tiedon avoimuudesta tehdään koko tietopolitiikan kantava periaate. Lähtökohtana muun muassa on, että julkiset toimijat avaavat julkiset rajapinnat, jos ei ole erityistä syytä pitää niitä suljettuina. Valtiovarainministeriön Tiedon hyödyntämisen ja avaamisen hanke toteuttaa pääministeri Marinin hallitusohjelman tietopolitiikkaan, tiedon hyödyntämiseen ja avaamiseen liittyviä tavoitteita[2]. Hanke on asetettu ajalle 30.4.2020–31.12.2022. Hankkeen tavoitteena on muun muassa edistää tietojen ja toiminnallisuuksien hyödyntämistä yhteneväisellä tavalla ohjelmointirajapintojen (API) kautta.

Tässä dokumentissa esitellään julkisen hallinnon ohjelmointirajapintojen (API) kehittämistä koskevat periaatteet ja tukimateriaali. Periaatteet muodostuvat suosituksista ja hyvistä käytänteistä julkisen hallinnon API-kehitykselle ja digitalisaation edistämiselle. Tukimateriaali ja esimerkit tarjoavat käytännönläheisiä ohjeita käyttöönoton tukemiseksi.

Periaatteet tukevat tiedonhallintalaissa[3] sähköiselle tietojen luovutustavalle säädettyjen vaatimusten toteuttamista. Periaatteiden viitekehyksenä on hyödynnetty Euroopan komission API Frameworkia[4] ja huomioitu muun muassa Euroopan yhteentoimivuusperiaatteet koskien teknistä ja semanttista yhteentoimivuutta[5]. Lisäksi periaatteiden ja tukimateriaalien valmistelussa on huomioitu sektorikohtainen sääntely, kuten INSPIRE-direktiivi[6],

1 Pääministeri Sanna Marinin hallituksen ohjelma (Valtioneuvosto, 2019:31)

2 Tiedon hyödyntämisen ja avaamisen hanke (Valtiovarainministeriö, 2021a)

3 Tiedonhallintalain 22§ ja 24§ (Tiedonhallintalaki 906/2019, 2019)

4 An Application Programming Interface (API) framework for digital government. (Joint Research Centre (European Commission), 2020)

5 Euroopan yhteentoimivuusperiaatteet –täytäntöönpanostrategia. (Euroopan Komissio, 2017)

6 INSPIRE-direktiivi (Euroopan parlamentin ja neuvoston direktiivi 2007/2/EY, 2019) ja kansallinen täytäntöönpano (Laki paikkatietoinfrastruktuurista 421/2009, 2009)

tiedonhallintalautakunnan antamat suositukset[7] sekä tiedon hyödyntämisen ja avaamisen kansalliset strategiset tavoitteet[8].

API-periaatteet ja tukimateriaali ottavat rajapintakehitykseen laajemmin kantaa kuin esimerkiksi tiedonhallintalautakunnan tämänhetkiset suositukset, jotka koskevat tiedonhallintalain piirissä olevia teknisiä rajapintoja[9]. API-periaatteet kattavat paitsi tietojen myös toiminnallisuuksien tarjoamisen ja hyödyntämisen sekä organisaation sisäisillä että ulkoisilla ohjelmointirajapinnoilla riippumatta käytetystä tiedonsiirtoprotokollasta.

Viranomaiset voivat jatkokehittää periaatteita omiin tarpeisiinsa, esimerkiksi velvoittavuuden osalta.

1.1 Tavoitteet

Periaatteiden tarkoituksena on edistää julkisen hallinnon tietojen ja toiminnallisuuksien tarjoamista sekä hyödyntämistä lähtökohtaisesti ohjelmointirajapintojen avulla. Periaatteiden tavoitteena on lisätä asiakaslähtöisyyttä, yhteistyötä, semanttista ja teknistä yhteentoimivuutta, uudelleenkäytettävyyttä, tietoturvan ja tietosuojan huomioimista sekä laatua ohjelmointirajapintojen kehityksessä.

Asiakaslähtöisyys tarkoittaa sitä, että ohjelmointirajapinnan potentiaalisten hyödyntäjien tarpeet huomioidaan ohjelmointirajapinnan koko elinkaaren ajan aina tarvekartoituksesta käytöstä poistoon asti. Asiakaslähtöisesti kehitettävät rajapinnat vastaavat hyödyntäjien tarpeisiin ja kehittyvät jatkuvasti hyödyntäjiä paremmin palvelevaan suuntaan. Asiakaslähtöisyys kasvattaa hyödyntäjien tyytyväisyyttä ja nostaa ohjelmointirajapintojen käyttöastetta.

Asiakaslähtöisyys vaatii **yhteistyötä** tiedon, toiminnallisuuksien ja rajapintojen tarjoajien sekä hyödyntäjien välillä. Yhteistyö voi olla organisaation sisäistä tai ulkoista yhteistyötä. Sisäinen yhteistyö kattaa oman organisaation eri tasojen, tiimien ja yksiköiden välisen yhteistyön. Ulkoinen yhteistyö voi olla julkisen sektorin toimijoiden välistä tai julkisen ja yksityisen sektorin toimijoiden välistä yhteistyötä tai yhteistyötä kansalaisten kanssa.

7 Tiedonhallintalataukunnan suositukset (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020–2021)

8 Strategiset tavoitteet ovat osa valtioneuvoston periaatepäätöstä tiedon hyödyntämiseksi ja avaamiseksi, joka on tarkoitus julkaista kevään 2022 aikana.

9 Tiedonhallintalautakunnan suositus teknisistä rajapinnoista ja katseluyhteyksistä (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:21)

Yhteistyö paitsi edistää asiakaslähtöistä kehittämistä myös mahdollistaa osaamisen, kokemuksien ja ratkaisuiden jakamisen eri toimijoiden välillä.

Uudelleenkäytettävyys tarkoittaa sitä, että ohjelmointirajapinnat ja niiden tarjoamat tiedot ja toiminnallisuudet ovat löydettävissä ja hyödynnettävissä uusien ratkaisujen toteutuksissa. Päällekkäinen työ ja päällekkäiset ratkaisut vähenevät, kehittämistyö nopeutuu ja tuottavuus kasvaa, kun uusia ratkaisuja voidaan kehittää jo olemassa olevien tietojen, toiminnallisuuksien ja ohjelmointirajapintojen päälle.

Tekninen yhteentoimivuus tarkoittaa tiedonsiirtotekniikoiden yhteensovittamista[10]. **Semanttinen yhteentoimivuus** tarkoittaa sitä, että eri toimijoiden välillä vaihdetun tiedon merkitys säilytetään ja ymmärretään osapuolten välillä sellaisena kuin se on lähetetty[11]. Teknisesti ja semanttisesti yhteentoimivien ohjelmointirajapintojen avulla tietojen liikutettavuus paranee, kehittämistyö nopeutuu ja tuottavuus kasvaa.

Tietoturvalla tarkoitetaan sitä, että käsiteltävien tietojen eheys, luottamuksellisuus ja saatavuus huomioidaan koko ohjelmointirajapinnan elinkaaren ajan. **Tietosuojalla** tarkoitetaan sitä, että ohjelmointirajapinnoissa käsiteltävät henkilötiedot on suojattu asetettujen vaatimuksien mukaisesti.

Laadulla tarkoitetaan sitä, että ohjelmointirajapintojen ominaisuudet tai kyvykkyydet täyttävät hyödyntäjiensä tarpeet ja odotukset[12]. Laadukkaiden ohjelmointirajapintojen avulla hyödyntäjien tyytyväisyys lisääntyy ja ohjelmointirajapintojen käyttöaste kasvaa. Laatu myös nopeuttaa kehittämistyötä ja kasvattaa sitä kautta tuottavuutta.

1.2 Kohderyhmä

Periaatteiden kohderyhmää ovat:

- Julkisen hallinnon organisaatiot, kuten valtion virastot ja laitokset, kunnat ja kuntayhtymät, hyvinvointialueet sekä korkeakoulut ja muut oppilaitokset.
- Yritykset, yhteisöt tai muut toimijat, jotka käsittelevät julkisen hallinnon tietoja tai toteuttavat julkista hallintotehtävää.
- Yritykset, yhteisöt tai muut toimijat, jotka toimittavat julkisen hallinnon organisaatiolle tietojenkäsittelyyn tai tiedonhallintaan liittyviä palveluita tai ratkaisuja.

10 Teknisen yhteentoimivuuden määritelmä (Valtiovarainministeriö, 2021b)
11 Semanttisen yhteentoimivuuden määritelmä (Valtiovarainministeriö, 2021b)
12 Laadun määritys perustuu OECD:n ISO-määritelmään (OECD, 2002)

1.3 Rajaukset

Periaatteet eivät koske loppukäyttäjille tarkoitettuja käyttöliittymärajapintoja.

Periaatteet eivät ole kaiken kattava ohjelmointirajapintojen käsikirja tai suunnitteluopas. Periaatteissa ei nimetä käytettäviä teknologioita, tiedonsiirtomuotoja tai tietomalleja, mutta annetaan niistä ohjeellisia esimerkkejä.

Periaatteet eivät myöskään sisällä toimialakohtaisia ohjeita tai määrityksiä, vaan niitä voidaan toimialoittain kehittää periaatteiden päälle.

2 Mitä API:t ovat?

2.1 Määritelmä

Ohjelmointirajapinnat eli API:t (Application Programming Interface) ovat dokumentoituja rajapintoja, joiden avulla ohjelmistot, sovellukset tai järjestelmät voivat vaihtaa keskenään tietoa tai toiminnallisuuksia[13]. Tässä dokumentissa API:lla, ohjelmointirajapinnalla ja tiedonhallintalaissa[14] määritellyllä teknisellä rajapinnalla tarkoitetaan samaa asiaa.

Näin määriteltynä ohjelmointirajapinta kattaa sekä web-pohjaiset REST, SOAP tai GraphQL API:t että tiedosto- tai tietokantapohjaisiin tai muihin protokolliin perustuvat rajapinnat. Olennaista on, että **ohjelmointirajapinta tarjoaa tietoa tai toiminnallisuutta koneluettavassa, dokumentoidussa muodossa siten, että jokin toinen ohjelmisto, sovellus tai järjestelmä voi sitä ohjelmallisesti hyödyntää**.

Huomioitavaa on se, että ohjelmointirajapinnalla ei tarkoiteta loppukäyttäjille tarkoitettuja käyttöliittymärajapintoja, vaan ohjelmointirajapinnan hyödyntäjä on aina jokin toinen ohjelmisto, sovellus, sovelluskomponentti tai järjestelmä.

2.2 Arvoketju

Ohjelmointirajapinnat voidaan nähdä omina tuotteinaan, joihin liittyy arvoketju[15] (kuva 1).

Arvoketju alkaa **digitaalisen hyödykkeen tarjoajasta**, jolla on hallussaan tuote, digitaalinen hyödyke, josta on muulle toimijalle arvoa. Digitaalinen hyödyke voi olla esimerkiksi tietoa, kuten tilasto- tai rekisteritietoa tai toiminnallisuutta, kuten veroprosentin laskenta, viitekehysmuunnin tai tietojen ilmoittamistoiminnallisuus.

Ohjelmointirajapinnan tarjoaja tarjoaa ohjelmointirajapinnan, jonka kautta muut toimijat voivat hyödyntää digitaalisen hyödykkeen tarjoajan tuotetta. Ohjelmointirajapinnan tarjoaja voi olla sama toimija tai eri toimija kuin digitaalisen hyödykkeen tarjoaja.

---

13 Määritys mukailee Euroopan Unionin julkaisun määritystä, s18–19 (Vaccari, et al., 2020)

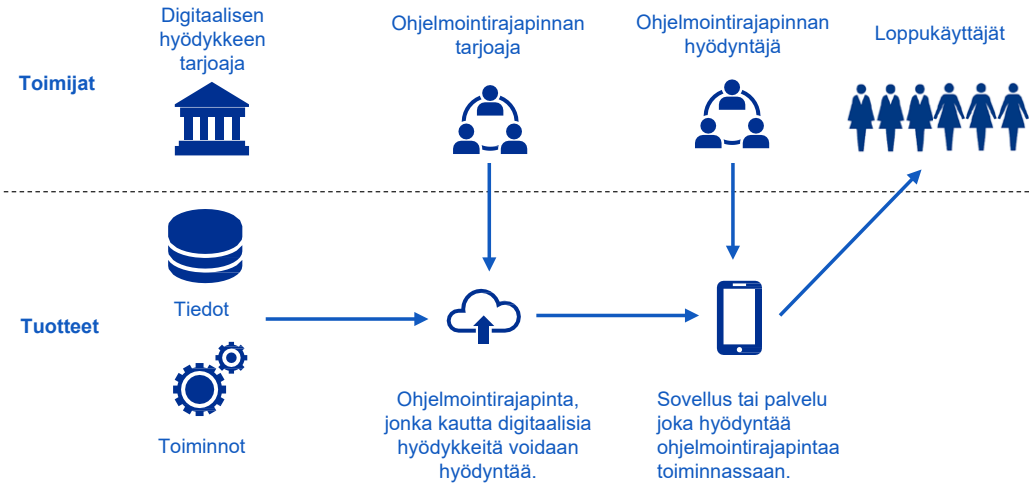
14 Tiedonhallintalain 2§, kohta 11 (Tiedonhallintalaki 906/2019, 2019)

15 Arvoketju mukailee Euroopan Unionin julkaisussa esitettyä arvoketjua, s 20 (Vaccari, et al., 2020)

Ohjelmointirajapinnan hyödyntäjä hyödyntää rajapintaa ja sen tarjoamaa tietoa tai toiminnallisuutta omassa sovelluksessaan tai palvelussaan. Ohjelmointirajapinnan hyödyntäjä voi olla sama tai eri toimija kuin ohjelmointirajapinnan tarjoaja.

Sovelluksella tai palvelulla voi olla vielä **loppukäyttäjiä**. Loppukäyttäjät eivät siis hyödynnä suoraan varsinaisia ohjelmointirapintoja, vaan sovellusta tai palvelua, joka hyödyntää API:a toiminnassaan.

Kuva 1. API:n arvoketju[16]



16 Arvoketju mukailee Euroopan Komission julkaisussa esitetty arvoketjua, s20 (Vaccari, et al., 2020).

ESIMERKKI

- Verohallinnolla on hallussaan tieto henkilöiden veronumeroista ja voimassaolosta[17]. Verohallinto on digitaalisen hyödykkeen tarjoaja.
- Verohallinto on kehittänyt toiminnallisuutta tarjoavan ohjelmointirajapinnan[18], jonka kautta muut toimijat voivat tarkistaa ohjelmallisesti, onko jokin veronumero voimassa vai ei. Verohallinto on ohjelmointirajapinnan tarjoaja.
- Yksityisen sektorin toimija kehittää tietojärjestelmän, jonka avulla voidaan ylläpitää rakennustyömaille myönnettyjä kulkulupia. Tietojärjestelmä käy uuden kulkuluvan perustamisen yhteydessä varmistamassa, että henkilön veronumero on voimassa Verohallinnon tarjoaman ohjelmointirajapinnan avulla. Yksityisen sektorin toimija on tässä tapauksessa ohjelmointirajapinnan hyödyntäjä.
- Rakennusyrityksen työntekijät, esimerkiksi työmaapäälliköt käyttävät tietojärjestelmää kulkulupien hallinnassa. He ovat loppukäyttäjiä.
- Verohallinto tarjoaa myös web-käyttöliittymän, jonka avulla veronumeron voi käydä tarkistamassa manuaalisesti esimerkiksi web-selaimen tai mobiililaitteen avulla[19]. Tässä tapauksessa Verohallinto tarjoaa suoraan loppukäyttäjille suunnattua sovellusta tai palvelua. Mikäli Verohallinto hyödyntää omaa ohjelmointirajapintaansa web-käyttöliittymän veronumeron tarkistuksessa, Verohallinto on myös yksi oman ohjelmointirajapintansa hyödyntäjistä.

17 Verohallinnnon veronumerorekisteri (Verohallinto, 2021d)

18 Veron Vero API (Verohallinto, 2021b)

19 Veron tarjoama web-käyttöliittymä (Verohallinto, 2021c)

2.3 Tyypitys

Ohjelmointirajapinnat voivat olla tyypiltään sisäisiä tai ulkoisia. Taulukossa 1 on esitelty ohjelmointirajapintojen eri tyypit ja niihin liittyvät yleiset ominaisuudet.

Taulukko 1. API-tyypit

Ohjelmointirajapinnan tyyppi		Käytön rajoitus	Potentiaalinen hyödyntäjä	Käsiteltävän tiedon luokittelu
SISÄINEN	Sisäinen API	Kyllä	Oman organisaation toimijat	Turvaluokiteltu tieto Salassa pidettävä tieto ml henkilötieto Julkinen tieto
ULKOINEN	Kumppani API	Kyllä	Oman organisaation toimijat Muut julkishallinnon toimijat Muut yksityisen sektorin toimijat Muut toimijat	Turvaluokiteltu tieto Salassa pidettävä tieto ml henkilötieto Julkinen tieto
	Julkinen API	Ei	Kuka tahansa	Julkinen tieto

Sisäiset ohjelmointirajapinnat (**sisäinen API**) ovat vain organisaation omaan käyttöön. Ulkoiset ohjelmointirajapinnat voivat olla rajoitettuja tietyille toimijoille (**kumppani API**) tai kaikille avoimia rajoittamattomia ohjelmointirajapintoja (**julkinen API**).

Sisäisissä tai ulkoisissa tietyille kumppaneille suunnatuissa ohjelmointirajapinnoissa voidaan käsitellä julkista tietoa, salassa pidettävää tietoa, henkilötietoa tai turvaluokiteltua tietoa. Julkisissa ohjelmointirajapinnoissa käsitellään vain julkista tietoa.

Sisäisissä ja tietyille kumppaneille rajoitetuissa ohjelmointirajapinnoissa yleensä rajapinnan hyödyntäjä tunnistetaan (autentikoidaan) ja hyödyntäjän käyttöoikeudet tarkistetaan (autorisoidaan). Julkisessa ohjelmointirajapinnassa käyttöoikeuksien tarkistusta (autorisointia) ei tarvita, koska tarjolla on vain julkista tietoa. Joissain tilanteissa hyödyntäjän tunnistus (autentikointi) voidaan julkisissakin ohjelmointirajapinnoissa tehdä; esimerkiksi jos halutaan kerätä tietoa ohjelmointirajapinnan hyödyntäjistä seurantaa tai viestintää varten.

ESIMERKKI

- Toimijalla, kuten kunnalla, valtion virastolla tai oppilaitoksella, voi olla omia rekistereitä, esimerkiksi asiakasrekisteri tai oppilasrekisteri. Toimija kehittää rekisterin tietojen hakua varten ohjelmointirajapinnan, jonka avulla toimijan muut tietojärjestelmät tai sovellukset voivat hakea ko. rekisteristä tietoja tiettyjen hakukriteerien avulla. Mikäli ohjelmointirajapinta on tarkoitettu vain toimijan omaan käyttöön, on kyseessä **sisäinen API**.
- Maanmittauslaitos tarjoaa kyselypalvelun[20], jonka avulla voidaan kysellä rakennuksien tunnistetietoja, ominaisuustietoja sekä omistajatietoa. Palvelun käyttö vaatii Digi- ja väestötietoviranomaisen lupaa ja on näin ollen rajattu tietyille toimijoille. Kyseessä on **kumppani API**.
- Väylävirasto tarjoaa kaikille avoimia rajapintoja[21], joiden avulla pääsee lataamaan ja katselemaan tie-, rata-, ja vesiväyläverkkoon liittyviä paikkatietoaineistoja. Kyseessä on **julkinen API**, jonka käyttö ei vaadi rekisteröitymistä eikä tunnistautumista.

2.4 Elinkaari

Ohjelmointirajapinnoilla on elinkaari, joka alkaa siihen liittyvästä tarvekartoituksesta ja päättyy ohjelmointirajapinnan käytöstä poistoon. Elinkaari kattaa kaikki tällä välillä olevat vaiheet, joita ovat määrittely ja suunnittelu, kilpailutus ja hankinta, toteutus ja kehitys, käyttöönotto, ylläpito sekä käytöstä poisto[22]. Ohjelmointirajapinnan elinkaari on iteratiivinen, eli vaiheita toistetaan, kunnes ohjelmointirajapinta kaikkine versioineen on poistettu käytöstä.

Huomioitavaa on se, että ohjelmointirajapinnan elinkaari voi poiketa tarjoamansa tiedon tai toiminnallisuuden elinkaaresta. Ohjelmointirajapinnan elinkaari voi alkaa vasta myöhemmin kuin tarjoamansa tiedon tai toiminnallisuuden elinkaari. Voi olla, että tiedon tai toiminnallisuuden elinkaaressa ei tapahdu muutoksia, mutta ohjelmointirajapinnan ominaisuuksia tai toiminnallisuuksia kehitetään, siitä luodaan uusia versiota ja vanhoja versioita poistetaan käytöstä. Ohjelmointirajapinnan elinkaari voi myös päättyä ennen kuin sen tarjoaman tiedon tai toiminnallisuuden elinkaari päättyy esimerkiksi käyttötarpeen päättymisen tai teknologian vanhentumisen vuoksi.

---

20 Maanmittauslaitoksen kyselypalvelu (Maanmittauslaitos, 2021b)

21 Väyläviraston avoimet rajapinnat (Väylävirasto, 2021)

22 Mukailee tietojärjestelmän elinkaarta, s26 (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:65)

3 Periaatteet

Periaatteet on jaettu kolmelle tasolle: strateginen, taktinen ja operatiivinen.

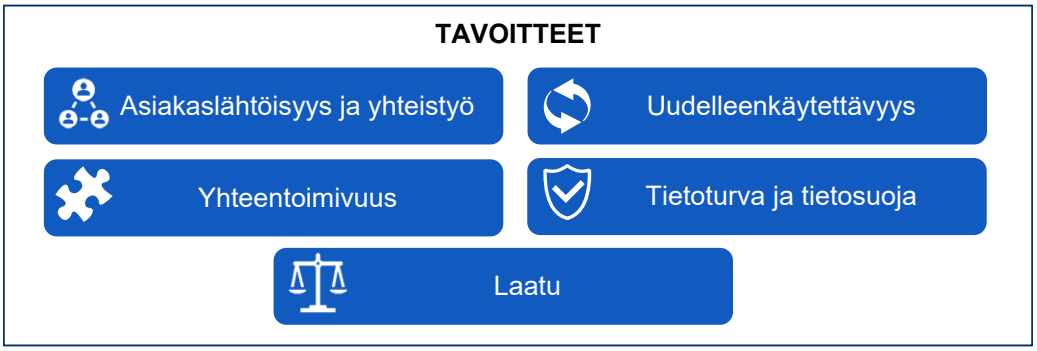
Strategisen tason periaatteet ovat kohdistettu organisaation johdolle. Strategisella tasolla kuvataan, miten ohjelmointirajapintojen kehittämiselle tulisi määrittää suunta ja tavoitteet ja miten ohjelmointirajapinnat tulisi huomioida toiminnan kehittämisessä.

Taktisen tason periaatteet ovat kohdistettu organisaation tiedonhallintaa kehittäville toimijoille. Taktisen tason periaatteet ohjaavat, miten ohjelmointirajapintojen kehittämistä ja ohjelmointirajapintojen muodostamaa kokonaisuutta tulisi hallita.

Operatiivisen tason periaatteet ovat kohdistettu ohjelmointirajapintoja kehittäville ja ylläpitäville toimijoille. Operatiivisen tason periaatteet ohjaavat, miten yksittäisiä ohjelmointirajapintoja tulisi kehittää ja ylläpitää.

Periaatteet ovat esitelty kappaleissa 3.1, 3.2 ja 3.3. Periaatteet tukevat asetettujen tavoitteiden saavuttamista (kuva 2). Periaatekohtaiset tavoitteet on kuvattu alla olevien symbolien avulla.

Kuva 2. Tavoitteet



3.1 Strateginen taso

Kuva 3. Strategisen tason periaatteet

Periaate 1.1 Tarjoa ja hyödynnä tietoja pääsääntöisesti ohjelmointirajapintojen kautta

Tunnista organisaatiosi toimintaprosessien ja ydintehtävien kannalta tärkeät tietoaineistot ja toiminnallisuudet, joita voidaan tarjota tai hyödyntää ohjelmointirajapintojen avulla. Tunnista myös niiden tuoma hyötypotentiaali. Huomioi, että tietoaineistot tai toiminnallisuudet voivat olla omia tai muiden toimijoiden. Tietoaineistojen ja toiminnallisuuksien hyötypotentiaali voi liittyä organisaation oman tai sidosryhmien toiminnan kehittämiseen tai tarpeeseen.

Ohjelmointirajapintojen kautta tarjottavia tai hyödynnettäviä tietoaineistoja tai toiminnallisuuksia voi määrittää esimerkiksi seuraavien kysymysten kautta:

- Mitä tietoa tai toiminnallisuuksia organisaatiollasi on saatavilla?
- Mitä tai millaista tietoa tarvitaan lisää?
- Millainen tieto tukee tiedolla johtamista?
- Mitkä ovat sidosryhmien tietojen tai toiminnallisuuksien tarpeet?
- Mitä tietoa tarvitaan säännöllisesti, koneluettavassa muodossa tai mahdollisimman ajantasaisena?
- Mitä toiminnallisuuksia olisi tarpeen tai mahdollista tarjota tai hyödyntää digitaalisesti?
- Pohdi myös millaisia hyötyjä, riskejä ja kustannuksia tietojen tai toiminnallisuuksien tarjoaminen ja hyödyntäminen aiheuttavat organisaatiollesi.

Määritä mitä tai millaisia tietoaineistoja tai toiminnallisuuksia voidaan tarjota tai hyödyntää ohjelmointirajapintojen avulla sisäisesti ja ulkoisesti. Tunnista tietojen tai toiminnallisuuksien hallinnoijat. Sisäinen tarjoaminen ja hyödyntäminen voidaan tehdä sisäisten rajapintojen (sisäinen API) avulla. Ulkoinen tarjoaminen ja hyödyntäminen voidaan tehdä kumppanirajapintojen (kumppani API) tai julkisten rajapintojen (julkinen API) avulla tiedon luokituksen mukaan. Julkiset rajapinnat voivat luoda uudenlaisia toimintatapoja, tuotoksia ja kumppanuuksia ja vaikuttaa siten merkittävästikin organisaatioiden toimintaan.

Huomioi tietojen saantioikeuksista, tietojen luovutuksista ja tietojen tarjoamisesta koneellisesti luettavassa muodossa säädetyt lait ja niiden asettamat velvoitteet[23]. On tärkeä myös tunnistaa ne tiedot, jotka ovat salassa pidettäviä. Huomioi myös tietoaineistoille mahdollisesti tarvittavat muokkaukset kuten pseudonymisointi tai anonymisointi[24].

---

23 Esimerkiksi Tiedonhallintalain 22§ (Tiedonhallintalaki 906/2019, 2019) ja Tiedonhallintalautakunnan suositus teknisistä rajapinnoista ja katseluyhteyksistä (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:21).

24 Pseudonymisoidut ja anonymisoidut tiedot -sivusto (Tietosuojavaltuutetun toimisto, 2021). Tutustu myös Kyberturvallisuuskeskuksen Tunnisteet ja tietosuoja, anonymisointi ja sen rajat -oppaaseen (Traficom, Kyberturvallisuuskeskus 2021)

TUOTOKSET

- Listaus mahdollisesti rajapintojen kautta tarjottavista tai hyödynnettävistä tietoaineistoista.
- Listaus mahdollisesti rajapintojen kautta tarjottavista tai hyödynnettävistä toiminnallisuuksista.

HYÖDYT

- Listausten avulla organisaation on helpompi tunnistaa ja kohdentaa rajapintakehittämistä hyötypotentiaalia omaaviin tietoaineistoihin ja toiminnallisuuksiin ja edistää sitä kautta tarvelähtöistä rajapintakehittämistä.
- Kohdennetulla ja tarvelähtöisellä kehittämisellä edistetään rajapintojen asiakaslähtöisyyttä ja yhteistyötä, uudelleenkäytettävyyttä, yhteentoimivuutta ja laatua.

TUKIMATERIAALI

Esimerkkejä tietoa tai toiminnallisuutta tarjoavista ohjelmointirajapinnoista:

- Helsingin kaupunki on avannut palauterajapinnan[25], jonka avulla voi antaa Helsingin kaupungille palautetta, kuten ilmoittaa rikkoutuneesta liikennemerkistä tai kuopista teissä ja lisäksi hakea järjestelmässä julkaistuja palautteita. Kyseessä on sekä toiminnallisuutta, palautteen antamista että tietoa tarjoava rajapinta.
- Finna tarjoaa avoimen rajapinnan[26], jonka avulla voi kohdistaa hakuja suomalaisten kirjastojen, arkistojen ja museoiden aineistoihin. Kyseessä on tietoa tarjoava rajapinta.

Tutustu myös seuraaviin aineistoihin, joista voit saada apua ohjelmointirajapintojen kautta tarjottavien tai hyödynnettävien tietojen ja toiminnallisuuksien tunnistamiseen ja hyötypotentiaalin arvioimiseen:

- Tiedonhallintalautakunnan julkaisema Suositus tiedonhallintamallista[27].
- Arviointimenetelmä hyötypotentiaalisten tietojen tunnistamiseen (hyödyt, riskit ja kustannukset) ja jakamiseen[28].
- Tiedonhallintakartta julkisen hallinnon yhteisten tietovarantojen lakisääteisten tietojen luovutusten nykytilan tunnistamiseen[29].

Periaate 1.2 Määritä ohjelmointirajapintojen tarjoamiselle ja hyödyntämiselle tavoitteet ja mittarit sekä hanki riittävät resurssit

Määritä ohjelmointirajapintojen tarjoamiselle ja hyödyntämiselle tavoitteet. Tavoitteiden tulee palvella organisaation strategiaa, toimintaprosesseja ja niiden tulee olla linjassa muun tiedonhallinnan tavoitteiden kanssa. Tavoitteiden tulee olla realistisia organisaation kokoon ja kyvykkyyksiin nähden. Tavoitteet voidaan kuvata

25 Helsingin kaupungin palauterajapinta (Helsingin kaupunginkanslia, 2020), tutustu myös 6Aika hankkeen tekemään määritelmään palauterajapinnasta (6Aika-kaupungit, 2016)

26 Finnan avoin rajapinta (Kansalliskirjasto, Finna, 2021)

27 Suositus Tiedonhallintamallista (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:29)

28 Arviointimenetelmä julkaistaan maaliskuussa 2022 Digi- ja väestötietoviraston ylläpitämässä avoindata.fi -palvelussa.

29 Julkisen hallinnon tiedonhallintakartta tutkihallintoa.fi -palvelussa (Valtiovarainministeriö, 2022)

esimerkiksi osana muita tiedonhallinnan tavoitteita tai datastrategiaa tai erillisessä API- tai integraatiostrategiassa.

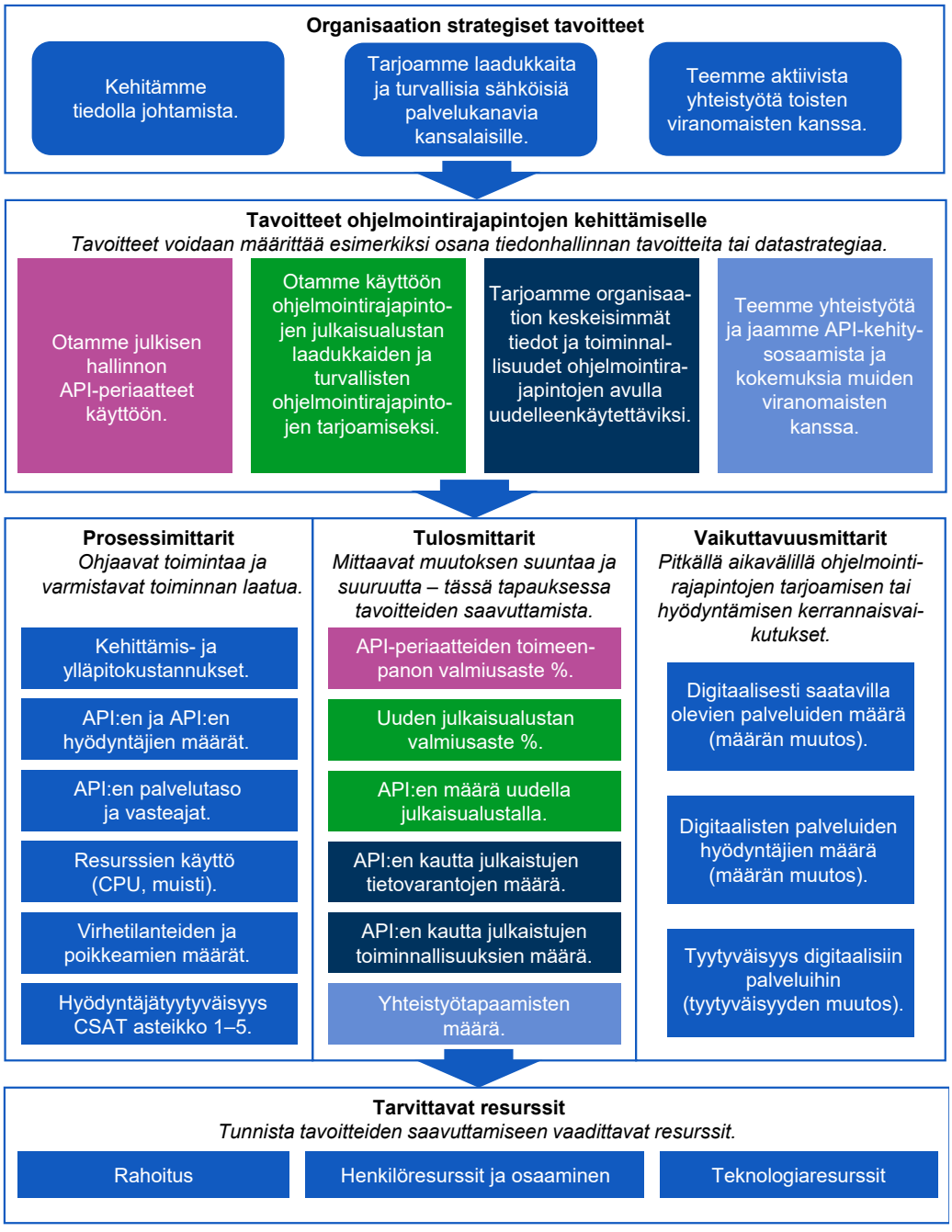
Määritä ohjelmointirajapintojen tarjoamiselle ja hyödyntämiselle tarvittavat mittarit. Mittarit voivat olla prosessi-, tulos- tai vaikuttavuusmittareita[30] (katso kuva 4). Prosessimittarien avulla ohjataan toimintaa tai varmistetaan toiminnan laatua, esimerkiksi palvelutason toteutumista. Tulosmittareilla mitataan yleensä jonkin muutoksen suuntaa ja suuruutta, esimerkiksi ohjelmointirajapinnoille asetettujen tavoitteiden saavuttamista. Vaikuttavuusmittarit kertovat toiminnan tuloksista suhteessa yhteiskunnalliseen päämäärään, ongelmaan tai tarpeeseen, esimerkiksi ohjelmointirajapintojen vaikutusta julkisen hallinnon palveluiden kehittymiseen tai tiedolla johtamiseen. Valitse sellaiset mittarit, jotka palvelevat organisaatiosi seurannan tarpeita ja joita on mahdollista seurata. Mittareita voidaan seurata organisaation eri tasoilla: strategisella, taktisella ja operatiivisella.

Hanki tavoitteiden saavuttamista varten tarvittavat resurssit. Huomioi resursseissa sekä ohjelmointirajapintojen tarjoaminen ja hyödyntäminen että ylläpitäminen. Resurssit voivat olla esimerkiksi henkilöresursseja, oikeanlaista osaamista tai teknologisia resursseja. Resurssien ja osaamisen hankkiminen ja ylläpitäminen vaativat rahoitusta. Käy keskustelua organisaation tiedonhallinnasta vastaavien tiimien tai henkilöiden kanssa osaamis-, resurssi- ja rahoitustarpeista niiden tunnistamista ja hankkimista varten. Kehitä mahdollisuuksien mukaan oman organisaatiosi henkilöstön osaamista. Hyödynnä jo olemassa olevia tiedonhallinnan, kokonaisarkkitehtuurin, sovelluskehityksen tai integraatioiden parissa työskenteleviä tiimejä tai henkilöitä.

Kuvassa 4 on esimerkki ohjelmointirajapintojen kehittämiselle asetetuista tavoitteista, mittareista ja tarvittavista resursseista. Esimerkkikuvassa ohjelmointirajapintojen kehittämisen tavoitteet on johdettu kuvitteellisen organisaation strategisista tavoitteista.

30 Mittareiden valinta (Hyvän Mitta, 2021)

Kuva 4. Esimerkki tavoitteista, mittareista ja resursseista



TUOTOKSET

- Ohjelmointirajapintojen kehittämisen tavoitteet. Voivat olla esimerkiksi osana tiedonhallinnan tavoitteita, datastrategiaa tai integraatiostrategiaa.
- Ohjelmointirajapintojen kehittämisen mittarit, jotka palvelevat organisaation seurannan tarpeita ja joita on mahdollista seurata.
- Resurssisuunnitelma tavoitteiden saavuttamista varten huomioiden henkilö- ja teknologiaresurssit sekä rahoituksen.

HYÖDYT

- Tavoitteiden asettamisen ja resurssisuunnitelman avulla organisaatio voi vaiheistaa ja priorisoida rajapintakehitystään ja kohdentaa resursseja kehitykseen, jolloin kehittäminen tapahtuu hallitusti, suunnitelmallisesti ja palvelee organisaation muita tavoitteita.
- Erilaisten mittareiden avulla organisaatio voi seurata ohjelmointirajapintojen kehityksessä tapahtunutta muutosta ja asetettujen tavoitteiden saavuttamista.
- Hallitulla ja suunnitelmallisella kehityksellä ja seurannalla edistetään rajapintojen uudelleenkäytettävyyttä, yhteentoimivuutta, tietoturvan ja tietosuojan huomioimista sekä laatua.

TUKIMATERIAALI

Esimerkkejä ohjelmointirajapintojen tarjoamiseen ja hyödyntämiseen liittyvistä tavoitteista ja tavoitteiden suhteuttamisesta organisaation muuhun strategiaan:

- Helsingin kaupungin datastrategia[31], joka ottaa kantaa tietojen tarjoamiseen ja hyödyntämiseen ohjelmointirajapintojen avulla.
- API-kehittäminen Verolla[32], joka esittelee ohjelmointirajapinnat Verohallinnon strategiassa.
- API:t osana valtioneuvoston periaatepäätöksen tiedon hyödyntämiseksi ja avaamiseksi strategisia tavoitteita.[33]

Tutustu myös seuraaviin aineistoihin, joista voit saada apua tavoitteiden ja mittareiden tunnistamista varten:

- Hyvän Mitta - hanke[34], sisältää lisätietoa vaikuttavuudesta, vaikuttavuusketjusta ja mittarien valinnasta.
- Metropolian opinnäytetyö: Strategisten tavoitteiden toteutumisen mittaaminen[35], sisältää mm. ”hyvän mittarin tunnusmerkit” -tarkastuslistan ja tietotekniikkaohjelmiston mittaristoesimerkin.

Periaate 1.3 Varmista hankinnoissa yhteentoimivuus muiden tietojärjestelmien kanssa

Varmista, että hankittavissa tietojärjestelmissä on ominaisuudet, jotka mahdollistavat tietojen tarjoamisen ja hyödyntämisen avointen ja teknologiariippumattomien ohjelmointirajapintojen kautta. Tarvittavia ominaisuuksia ovat esimerkiksi:

- Valmisohjelmiston tarjoamat valmiit ohjelmointirajapinnat, joiden avulla voidaan tarjota järjestelmän sisältämiä tietoja tai toiminnallisuuksia muille järjestelmille. Ohjelmointirajapintojen tulisi perustua avoimiin, teknologiariippumattomiin ja yleisesti käytössä oleviin protokolliin ja standardeihin.

31 Helsingin kaupungin datastrategia, luku 5 (Digitaalinen Helsinki, 2021)

32 Veron API-kehittäminen (Verohallinto, 2019)

33 Valtioneuvoston periaatepäätös tiedon hyödyntämiseksi ja avaamiseksi on tarkoitus julkaista kevään 2022 aikana.

34 Hyvän Mitta (Hyvän Mitta, 2021)

35 Strategisten tavoitteiden toteutumisen mittaaminen (Rautio, 2015)

- Välineet, joiden avulla voidaan kehittää kokonaan uusia rajapintoja tai muokata valmiita rajapintoja paremmin tarkoitukseen soveltuviksi.
- Välineet, joiden avulla voidaan integroida järjestelmä muiden järjestelmien tarjoamiin rajapintoihin.
- Lisensointimalli tai -ehdot, jotka mahdollistavat järjestelmän tietojen ja toiminnallisuuksien tarjoamisen, hyödyntämisen ja uudelleenkäyttämisen organisaation sisäisesti sisäisten rajapintojen (sisäinen API) että ulkoisesti ulkoisten rajapintojen (kumppani API, julkinen API) avulla.
- Käyttöoikeuksien ja käyttötarkoituksen hallinta salassa pidettävien, turvallisuusluokiteltujen ja henkilötietojen vaatimusten mukaisuuden varmistamiseksi.

Tietojärjestelmähankinnoissa tietojen ja toiminnallisuuksien tarjoamiseen ja hyödyntämiseen liittyvät **vaatimukset pitää sisällyttää jo tarjouspyynnössä osaksi hankittavan kohteen määrittelyä**[36]. Organisaation tietohallinnon on tärkeää olla alusta alkaen mukana uusissa tietojärjestelmähankinnoissa.

TUOTOKSET

- Ohjelmointirajapintojen vaatimukset osana hankinnan kohteen kuvausta.

HYÖDYT

- Huomioimalla tietojen ja toiminnallisuuksien tarjoamiseen ja hyödyntämiseen liittyvät vaatimukset jo tietojärjestelmien hankintavaiheessa mahdollistetaan tietojärjestelmän yhteensovittaminen organisaation nykyiseen tietojenkäsittely-ympäristöön ja siihen jatkossa tuleviin muutoksiin.
- Lisäksi avoimet, teknologiariippumattomat ja yleisesti käytössä protokollat ja standardit sekä joustava lisensointimalli vähentävät mahdollisen toimittajalukon riskiä.
- Tietojärjestelmät, jotka kykenevät tarjoamaan ja hyödyntämään avoimia, teknologiariippumattomia ja yleisesti käytössä olevia ohjelmointirajapintoja edistävät niiden uudelleenkäytettävyyttä sekä teknistä yhteentoimivuutta.

36 Hankintalaki (Laki julkisista hankinnoista ja käyttöoikeussopimuksista 1397/2016, 2016).

TUKIMATERIAALI

Tukea ja lisätietoa hankintoihin liittyen saa esimerkiksi:

- Julkisten hankintojen neuvontayksikön verkkopalvelusta[37].
- HANSEL:in ylläpitämistä yhteishankintamateriaaleista[38].
- Tiedonhallintalautakunnan suosituskokoelmasta tiettyjen tietoturvallisuussäännösten soveltamisesta[39], jossa otetaan kantaa tiedon elinkaaren huomioimisesta tietojärjestelmissä mukaan lukien kilpailutus- ja hankintavaihe.

Periaate 1.4 Edistä sisäistä ja ulkoista yhteistyötä

Tunnista ohjelmointirajapintojen tarjoamiseen ja hyödyntämiseen liittyvät sisäiset ja ulkoiset yhteistyötarpeet. Yhteistyötarpeet voivat liittyä esimerkiksi:

- Ideoiden tai tarpeiden tunnistamiseen tai jakamiseen.
- Tavoitteiden, toimintamallien, ohjeiden tai ohjeistusten kehittämiseen tai jakamiseen.
- Ratkaisuiden kehittämiseen tai jakamiseen.
- Osaamisen tai kokemusten jakamiseen.

Tunnista sidosryhmät, joiden kanssa yhteistyötä tulisi tehdä. Huomioi, että yhteistyötä tehdään organisaatioiden eri tasoilla. Sidosryhmiä ovat esimerkiksi:

- Oman tai muun organisaation johto.
- Oman tai muun organisaation tiedonhallintaa kehittävät henkilöt tai tiimit.
- Oman tai muun organisaation kehitys- ja ylläpitotiimit.

Määritä omasta organisaatiosta ne henkilöt tai tiimit, joiden tulisi yhteistyötä edistää tai yhteistyöhön osallistua. Pohdi yhdessä heidän kanssaan minkälaisella yhteistyörakenteella voisitte edistää ja tehostaa tiedon ja toiminnallisuuksien hyödyntämistä niin organisaation sisällä kuin ulkopuolella rajapintojen kautta. Pienissä organisaatioissa tämä

37 Julkisten hankintojen neuvontayksikkö (Julkisten hankintojen neuvontayksikkö, 2021)

38 Yhteishankinnat (Hansel, 2021)

39 Tiedonhallintalautakunnan suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:65)

voi tarkoittaa vain paria henkilöä, jolloin on erityisesti syytä tehdä yhteistyötä ja jakaa kehittäjäkokemuksia verkostoissa.

Määritä ja ota käyttöön tarvittavat yhteistyömenetelmät. Huomioi jo olemassa olevat yhteistyöverkostot ja –foorumit.

TUOTOKSET

- Suunnitelma yhteistyöstä sisältäen sisäiset ja ulkoiset sidosryhmät ja yhteistyömenetelmät.
- Yhteistyön tuotokset, esimerkiksi tunnistetut tarpeet, jaetut ratkaisut tai kokemukset sekä osaamisen kehittyminen.

HYÖDYT

- Verkostoitumisen, yhteistyön ja jatkuvan keskustelun avulla kyetään tunnistamaan organisaatioiden sisäisten ja ulkoisten sidosryhmien muuttuvia tarpeita ja kehittämään tarpeisiin vastaavia ohjelmointirajapintoja.
- Lisäksi yhteistyö mahdollistaa osaamisen jakamisen yli organisaatiorajojen, kun jo saatuja oppeja, kokemuksia ja ratkaisuja jaetaan eri toimijoiden kesken.
- Sidosryhmien tarpeiden tunnistaminen edistää ohjelmointirajapintojen asiakaslähtöisyyttä ja yhteistyötä, uudelleenkäytettävyyttä, yhteentoimivuutta ja laatua.

TUKIMATERIAALI

Esimerkkejä olemassa olevista yhteistyöfoorumeista, joihin organisaation henkilöstö voi liittyä:

- Avoimen tiedon verkosto[40]
- Maanmittauslaitoksen yhteistyöryhmät[41]
- Verkkolaskufoorumi[42]
- API-Suomi Facebook-ryhmä[43]
- Github-yhteisöt[44]
- Suomen standardisoimisliitto SFS Ry:n tieto-ja viestintätekniikan standardisointiryhmät[45].

40 Avoimen tiedon verkosto (Varsinais-Suomen liitto, 2021)

41 Maanmittauslaitoksen yhteistyöryhmät (Maanmittauslaitos, 2021c)

42 Verkkolaskufoorumi (TIEKE Tietoyhteiskunna Kehittämiskeskus Ry, 2021)

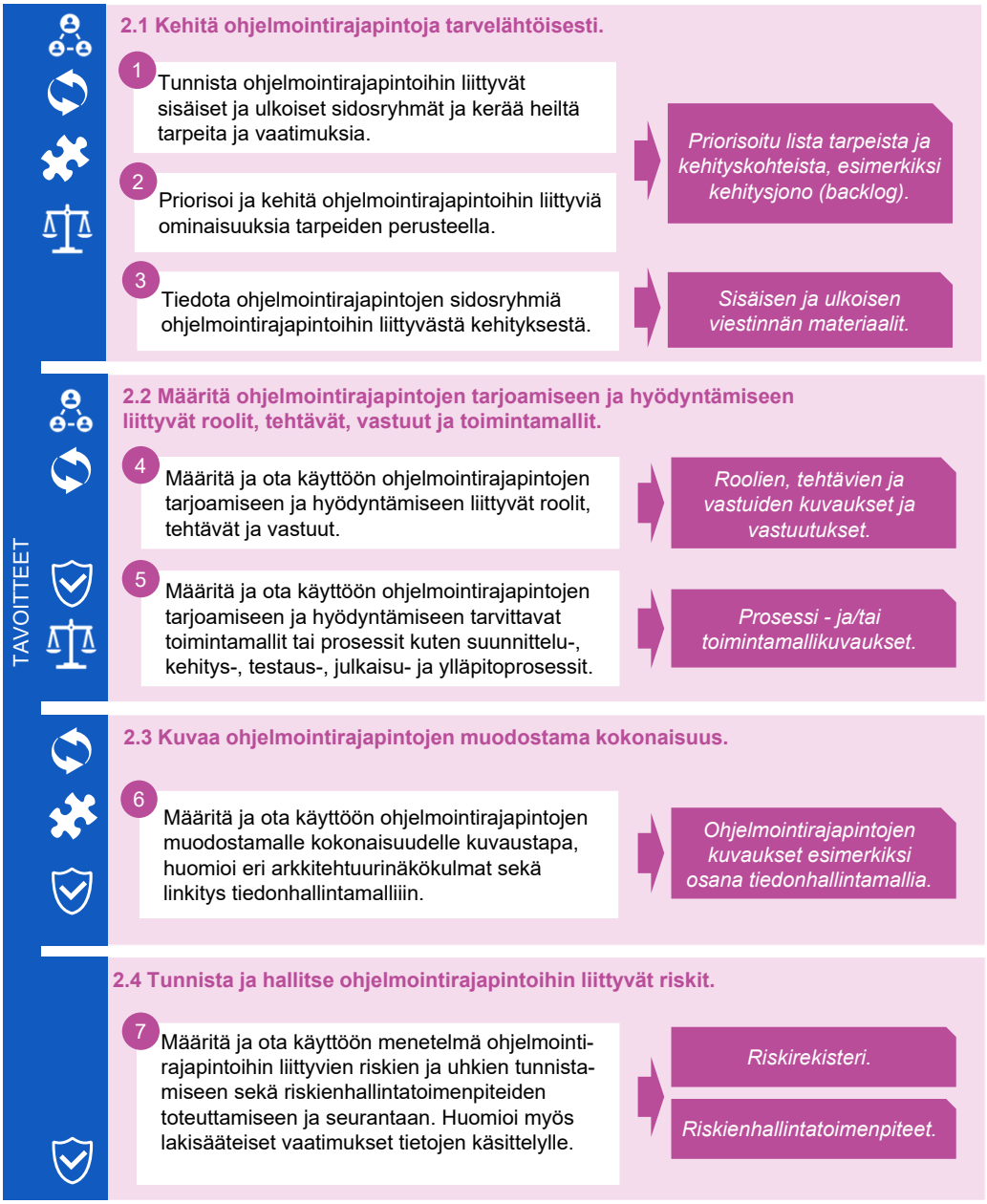
43 API-Suomi Facebook-ryhmä (Honkanen, 2021)

44 GIT-hubin yhteisöt (GitHub, 2021)

45 Tieto -ja viestintätekniikan standardisointiryhmät (Suomen standardisoimisliitto SFS Ry, 2021b)

3.2 Taktinen taso

Kuva 5. Taktisen tason periaatteet



Periaate 2.1 Kehitä ohjelmointirajapintoja tarvelähtöisesti

Tunnista ohjelmointirajapintoihin liittyvät sisäiset ja ulkoiset sidosryhmät ja kerää heiltä tarpeita ja vaatimuksia. Sidosryhmiä ovat esimerkiksi:

- Arvoketjuun liittyvät toimijat, kuten digitaalisen hyödykkeen tarjoaja, ohjelmointirajapinnan tarjoaja sekä ohjelmointirajapinnan hyödyntäjä tai potentiaalinen hyödyntäjä.
- Oman tai muun toimijan tiedonhallinnan parissa työskentelevät henkilöt, tiimit tai ryhmät, johto, suunnittelijat, kehittäjät, testaajat tai ylläpitäjät.

Tarpeet voivat liittyä rajapintojen toiminnallisuuksiin tai ei-toiminnallisuuksiin kuten saatavuuteen, käytettävyyteen, tiedon eheyteen, palvelutasoon tai kehittäjä- tai loppukäyttäjäkokemukseen. Huomioi myös lainsäädännöstä tulevat vaatimukset[46] **ja lainsäädännössä tapahtuvat muutokset**. Tarpeita voidaan kerätä muun muassa hyödyntämällä kyselyitä, palautekanavia, yhteistyöryhmiä, työpajoja tai muita yhteistyömenetelmiä. Jos kyseessä on julkinen tai avoimen datan rajapinta, jonka hyödyntäjiä ei kyetä tunnistamaan, saattaa tarpeiden keruu hyödyntäjiltä tai potentiaalisilta hyödyntäjiltä olla hankalaa. Tällaisessakin tapauksessa voidaan esimerkiksi julkaista avoin palautekanava hyödyntäjiä varten.

Priorisoi ja kehitä ohjelmointirajapintoihin liittyviä ominaisuuksia tarpeiden perusteella. Huomioi tarpeet ohjelmointirajapintojen koko elinkaaren ajan aina tarvekartoituksesta käytöstä poistoon asti: määrittele ja suunnittele, kilpailuta ja hanki, toteuta ja kehitä, käyttöönota, ylläpidä ja poista ohjelmointirajapintoihin liittyviä ominaisuuksia tarpeiden ja vaatimusten mukaisesti.

Tiedota ohjelmointirajapintojen sidosryhmiä ohjelmointirajapintoihin liittyvästä kehityksestä. Huomioi viestinnässä sekä organisaation sisäiset että ulkoiset sidosryhmät.

46 Esimerkiksi tiedonhallintalain vaatimus toistuvan ja vakiosisältöisen sähköisen tietojen luovutuksesta teknisen rajapinnan avulla (Tiedonhallintalaki 906/2019, 2019) sekä turvallisuusluokiteltujen asiakirjojen käsittelylle asetetut lakivaatimukset (Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa, 1101/2019). Tutustu myös tiedonhallintalautakunnan suosituksiin (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020–2021).

TUOTOKSET

- Priorisoitu lista ohjelmointirajapintoihin liittyvistä tarpeista ja kehityskohteista, esimerkiksi kehitysjono (backlog).
- Sisäisen ja ulkoisen viestinnän materiaalit.

HYÖDYT

- Tarpeiden kerääminen ja tunnistaminen auttavat kohdistamaan ohjelmointirajapintojen kehitykseen tarvittavat resurssit ja toimenpiteet tehokkaasti niiden tarpeiden täyttämiseen, joista on eniten hyötyä niin organisaatiolle itselleen kuin ohjelmointirajapintojen hyödyntäjille.
- Ohjelmointirajapintojen kehittämisestä tiedottaminen antaa sidosryhmille mahdollisuuden reagoida ajoissa tuleviin muutoksiin sekä suunnitella omaa toimintaansa huomioiden suunnitteilla olevat kehityskohteet.
- Oikein kohdistetut resurssit, hyödylliset ja tarpeet täyttävät ohjelmointirajapinnat sekä aktiivinen viestintä edistävät ohjelmointirajapintojen asiakaslähtöisyyttä ja yhteistyötä, uudelleenkäytettävyyttä, yhteentoimivuutta ja laatua.

TUKIMATERIAALI

Esimerkkejä julkisen hallinnon organisaatioiden julkaisemista avoimista kanavista, joiden kautta kyetään keräämään tarpeita sidosryhmiltä tai viestimään sidosryhmille:

- Digitraffic-sivusto[47], jonka kautta pääsee näkemään rajapintojen tiloja ja rajapintoihin liittyviä tiedotteita. Lisäksi sivuilta on linkitys avoimiin Google-keskusteluryhmiin, joissa mm. tiedotetaan rajapintojen kehityksestä ja käyttökatkoista.
- Vero API -sivusto[48], joka tarjoaa muun muassa katsauksen suunnitteilla oleviin rajapintoihin sekä havaintolomakkeen, jonka avulla ohjelmointirajapintojen hyödyntäjät voivat antaa palautetta tai kehitysideoita Verohallinnolle.

47 Liikenteen avoin data ja rajapinnat (Fintraffic, 2021)

48 Vero API (Verohallinto, 2021b)

Periaate 2.2 Määritä ohjelmointirajapintojen tarjoamiseen ja hyödyntämiseen liittyvät roolit, tehtävät, vastuut ja toimintamallit

Määritä ja ota käyttöön ohjelmointirajapintojen tarjoamiseen ja hyödyntämiseen liittyvät roolit, tehtävät ja vastuut. Huomioi ohjelmointirajapintakonaisuuden hallintaan liittyvät tehtävät kuten tiedonhallintamallin ylläpito, riskienhallinta ja arkkitehtuuriohjaus sekä ohjelmointirajapintojen tarjoamiseen ja hyödyntämiseen liittyvät tehtävät sekä ohjelmointirajapinnassa käsiteltävien tietojen hallintavastuut. Hyödynnä mahdollisuuksien mukaan organisaatiossa jo olemassa olevia rakenteita ja hyviä käytäntöjä. Ohjelmointirajapintojen hyödyntäminen tarkoittaa käytännössä integraatiota johonkin ohjelmointirajapintaan. Ohjelmointirajapinnoilla ja integraatioilla on elinkaari, joten tehtävissä tulee huomioida elinkaaren eri vaiheet:

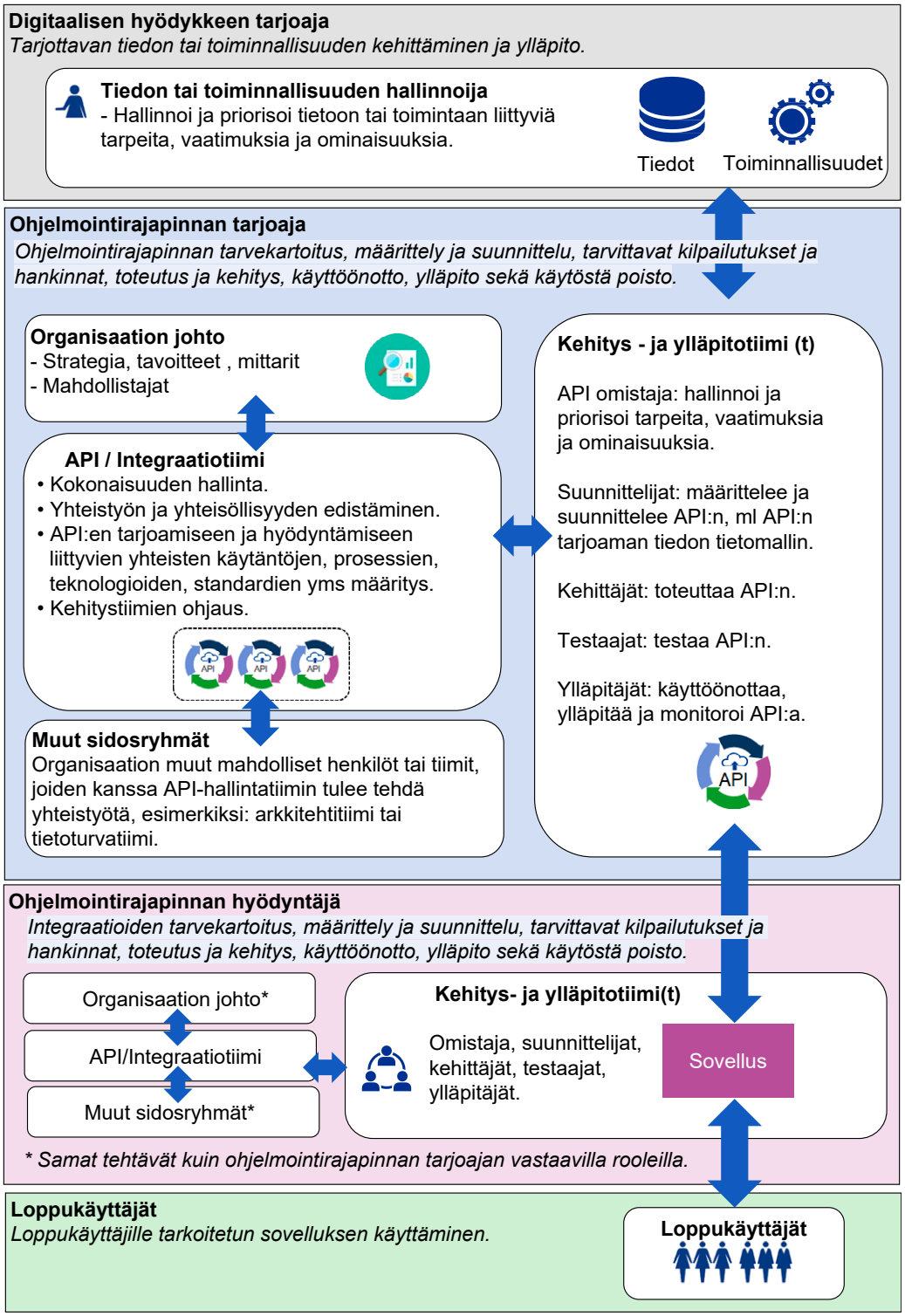
- Ohjelmointirajapinnan tai integraation tarpeiden kartoitus ja priorisointi.
- Ohjelmointirajapinnan tai integraation määrittely ja suunnittelu, tietoturva ja tietosuoja huomioiden.
- Ohjelmointirajapintaan tai integraatioon liittyvät kilpailutukset ja hankinnat.
- Ohjelmointirajapinnan tai integraation toteutus ja kehitys.
- Ohjelmointirajapinnan tai integraation käyttöönotto.
- Ohjelmointirajapinnan tai integraation ylläpito ja tuki.
- Ohjelmointirajapinnan tai integraation käytöstä poisto.

Osa ohjelmointirajapinnan elinkaareen liittyvistä tehtävistä voidaan ulkoistaa; esimerkiksi ohjelmointirajapintojen toteutusta ja kehitystä tai ylläpitoa ja tukea voidaan ulkoistaa kumppaneille. Huomioi rooli-, vastuu- ja tehtäväkuvauksissa oman organisaatiosi ja kumppaniesi roolit, tehtävät ja vastuut.

Määritä ja ota käyttöön ohjelmointirajapintojen tarjoamiseen ja hyödyntämiseen tarvittavat toimintamallit tai prosessit, kuten suunnittelu-, kehitys-, testaus-, julkaisu- ja ylläpitoprosessit. Huomio toimintamallien ja prosessien kuvaamisessa oman organisaation lisäksi myös toimintamalliin tai prosessiin keskeisesti liittyvät muut julkiset ja yksityiset organisaatiot.

Kuva 6 sisältää yhdenlaisen esimerkin API-arvoketjun eri toimijoista, toimijoiden rooleista, tehtävistä ja vastuista huomioiden sekä ohjelmointirajapintojen kokonaisuuden hallinnan että ohjelmointirajapintojen tarjoamisen ja hyödyntämisen. Esimerkin on tarkoitus auttaa hahmottamaan rooleja, tehtäviä ja vastuita paremmin. Isossa organisaatiossa tehtäviä voidaan allokoida eri henkilöille ja tiimeille. Pienessä organisaatiossa voi olla niin, että yksittäisille henkilöille tulee useita esimerkkikuvassa näkyvien tiimien tai roolien tehtäviä. Toimintamalleja miettiessä avainasemassa on organisaation koko ja jo olemassa oleva organisaatiorakenne.

Kuva 6. Esimerkki toimijoista, rooleista ja vastuista



TUOTOKSET

- Roolien, tehtävien ja vastuiden kuvaukset ja vastuujaot.
- Prosessi- ja/tai toimintamallikuvaukset.

HYÖDYT

- Ohjelmointirajapintoihin liittyvien roolien, tehtävien, vastuiden ja toimintamallien määrittäminen ja kuvaaminen auttavat organisaatiota ja ohjelmointirajapintojen hyödyntäjiä ymmärtämään millaisen API-arvoketjun osa ohjelmointirajapinta on / ohjelmointirajapinnat ovat.
- Koko elinkaaren huomioiminen määrityksissä ja kuvauksissa on tärkeää, jotta voidaan varmistaa kehittämiseen tarvittavien tehtävien lisäksi myös tuotannon jatkuvuuteen ja toipumiseen liittyvät tehtävät.
- API-arvoketjun ymmärtäminen ja ohjelmointirajapinnan koko elinkaaren huomioiminen edistävät ohjelmointirajapintojen asiakaslähtöisyyttä ja yhteistyötä, uudelleenkäytettävyyttä, tietoturvaa ja tietosuojaa sekä laatua.

TUKIMATERIAALI

Esimerkkejä ohjelmointirajapintojen ja integraatioiden kehittämiseen sopivista toimintamalleista tai menetelmistä:

- ApiOpsCycles, joka tarjoaa menetelmän ja työkaluja ohjelmointirajapintojen kehittämisen eri vaiheisiin[49].
- DevOps (Development and Operation), jonka periaatteita ovat ketterä kehitys, jatkuva integraatio, jatkuva toimitus ja automaatio[50].
- DevSecOps (Development, Security and Operation), joka laajentaa DevOpsia tuoden siihen tietoturvan vahvemmin jokaiseen vaiheeseen mukaan[51].

49 ApiOpsCycles (APIOps Cycles TM, 2021)

50 Useita eri lähteitä mm. (ite wiki, 2021) ja (DevOps.com, 2021)

51 Useita lähteitä, mm. DevSecOps Fundamentals, s. 17 (Department of Defence, United States of America, 2021) ja DevSecOps Manifesto (DevSecOps, 2021)

Periaate 2.3 Kuvaa ohjelmointirajapintojen muodostama kokonaisuus

Määritä ja ota käyttöön ohjelmointirajapintojen muodostamalle kokonaisuudelle kuvaustapa. Tärkeää on kyetä hallinnoimaan mitä ohjelmointirajapintoja tarjotaan, kenelle ja miksi sekä mitä ohjelmointirajapintoja hyödynnetään, keneltä ja miksi. Tarjottavat ja hyödynnettävät rajapinnat voivat olla organisaation omia sisäisiä rajapintoja (sisäinen API) tai ulkoisia rajapintoja (kumppani API, julkinen API). Ulkoisten rajapintojen tarjoajat tai hyödyntäjät voivat olla kansallisia toimijoita, kuten muu julkinen organisaatio tai yksityinen organisaatio tai kansainvälisiä toimijoita, kuten Euroopan unionin muu jäsenvaltio tai kansainvälinen kaupallinen organisaatio.

Periaate 3.3 Turvaa, testaa, versioi, dokumentoi ja julkaise ohjelmointirajapinnat määrittää, mitä yksittäisen ohjelmointirajapinnan dokumentaation tulee sisältää. Tämä periaate määrittää, mitä meta- ja viitetietoja ohjelmointirajapinnoista tulee kuvata ja hallinnoida osana tiedonhallintamallia, kokonaisarkkitehtuuria tai muuta kokonaiskuvausta.

Hyödynnä kokonaisuuden kuvaamisessa organisaatiossa käytössä olevia kokonais- ja ratkaisuarkkitehtuurin kuvauskäytäntöjä. Huomioi kuvauksissa eri arkkitehtuurinäkökulmat sekä linkitykset tiedonhallintamalliin[52]:

- Toiminta-arkkitehtuurin näkökulmasta ohjelmointirajapinnat osallistuvat jonkin prosessin tai toiminnallisuuden toteuttamiseen. Linkitys prosessiin voidaan tehdä esimerkiksi tietovarannon tai tietojärjestelmän kautta.
- Tietoarkkitehtuurin näkökulmasta ohjelmointirajapinnat käsittelevät jonkin tai joidenkin tietovarantojen tietoja.
- Tietojärjestelmäarkkitehtuurin näkökulmasta ohjelmointirajapinnat liittyvät johonkin tietojärjestelmään.
- Teknologia-arkkitehtuurin näkökulmasta ohjelmointirajapinnat hyödyntävät jotain tai joitain teknologiaresursseja.
- Integraatioarkkitehtuurin näkökulmasta ohjelmointirajapinnat liittyvät yhteen tai useampaan tietojärjestelmien väliseen liittymään eli tietovirtaan.
- Tietoturva-arkkitehtuurin näkökulmasta ohjelmointirajapinnat aiheuttavat tietoriskejä, jotka pitää tunnistaa ja hallita riskienhallintatoimenpiteiden avulla.
- Tiedonhallintamallin näkökulmasta ohjelmointirajapintojen kuvaukset syventävät tiedonhallintamallin kuvauksia[53]. Tiedonhallintamallista

52 Tiedonhallintalaki, 5§ (Tiedonhallintalaki 906/2019, 2019), tutustu myös suositukseen tiedonhallintamallista (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:29)

53 Suositus tiedonhallintamallista (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:29), tutustu myös suositukseen teknisistä rajapinnoista ja katseluyhteyksistä (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:21).

voidaan johtaa kuvaukset julkisen hallinnon tiedonhallintakarttaan[54] ja asiakirjajulkisuuskuvaukseen[55].

Ohjelmointirajapinnoista kuvattavia asioita ovat:

- Nimike: Nimi, tunniste tai muu yksilöivä tieto, jolla ohjelmointirajapinta voidaan erottaa muista ohjelmointirajapinnoista.
- Käyttötarkoitus: Lyhyt sanallinen kuvaus siitä, mihin ohjelmointirajapintaa käytetään.
- Omistaja: Henkilö tai tiimi, joka vastaa ohjelmointirajapinnan hallinnoinnista, tarpeista, vaatimuksista ja ominaisuuksista. Esimerkiksi jos ohjelmointirajapinta kuuluu osaksi jotain tietojärjestelmää, voi ohjelmointirajapinnan omistaja olla sama taho kuin tietojärjestelmän omistaja. Jos ohjelmointirajapinta on irrallinen, oma tuotteensa, tulee sillä olla selkeästi määritetty omistaja.
- Elinkaari: Elinkaaren tila, joka kuvaa sitä, missä elinkaarensa vaiheessa ohjelmointirajapinta on. Elinkaaren tilat voidaan johtaa ohjelmointirajapinnan elinkaaren eri vaiheista, joita ovat: määrittely ja suunnittelu, kilpailutus ja hankinta, toteutus ja kehitys, käyttöönotto, ylläpito, käytöstä poisto. Yksinkertaisimmillaan tilat voivat esimerkiksi olla: kehityksessä / käytössä / poistumassa käytöstä / poistettu käytöstä.
- Tietovirta: Linkitys niihin tietojärjestelmien välisiin liittymiin eli tietovirtoihin, joissa kyseistä ohjelmointirajapintaa hyödynnetään.
- Tarjoaja: Ohjelmointirajapinnan tarjoaja ja ohjelmointirajapintaan liittyvä tietojärjestelmä, jos sellaista on.
- Hyödyntäjät: Listaus ohjelmointirajapinnan hyödyntäjistä. Mikäli yksittäisiä hyödyntäjiä ei tiedetä tai tunnisteta, esimerkiksi jos kyseessä on kaikille avoin julkinen rajapinta, riittää, että kuvataan, kenelle ohjelmointirajapinta on tarkoitettu.
- Käsiteltävät tiedot: Mikäli ohjelmointirajapinta käsittelee jotain tietoa, suhde tietoon, tietovarantoon, tietoaineistoon tai tietoryhmään. Huomioi käsiteltävissä tiedoissa myös henkilötiedot ja salassa pidettävät tiedot.
- Teknologiat: Kuvaus siitä, mitä teknologiaresurssia ohjelmointirajapinta hyödyntää.

Kuvaukset tulee pitää ajantasaisina. Hyödynnä tietojen muodostamiseen tai ylläpitoon automatiikkaa mahdollisuuksien mukaan.

54 Julkisen hallinnon tiedonhallintakartta tutkihallintoa.fi -palvelussa (Valtiovarainministeriö, 2022)

55 Tiedonhallintalain 28§ (Tiedonhallintalaki 906/2019, 2019)

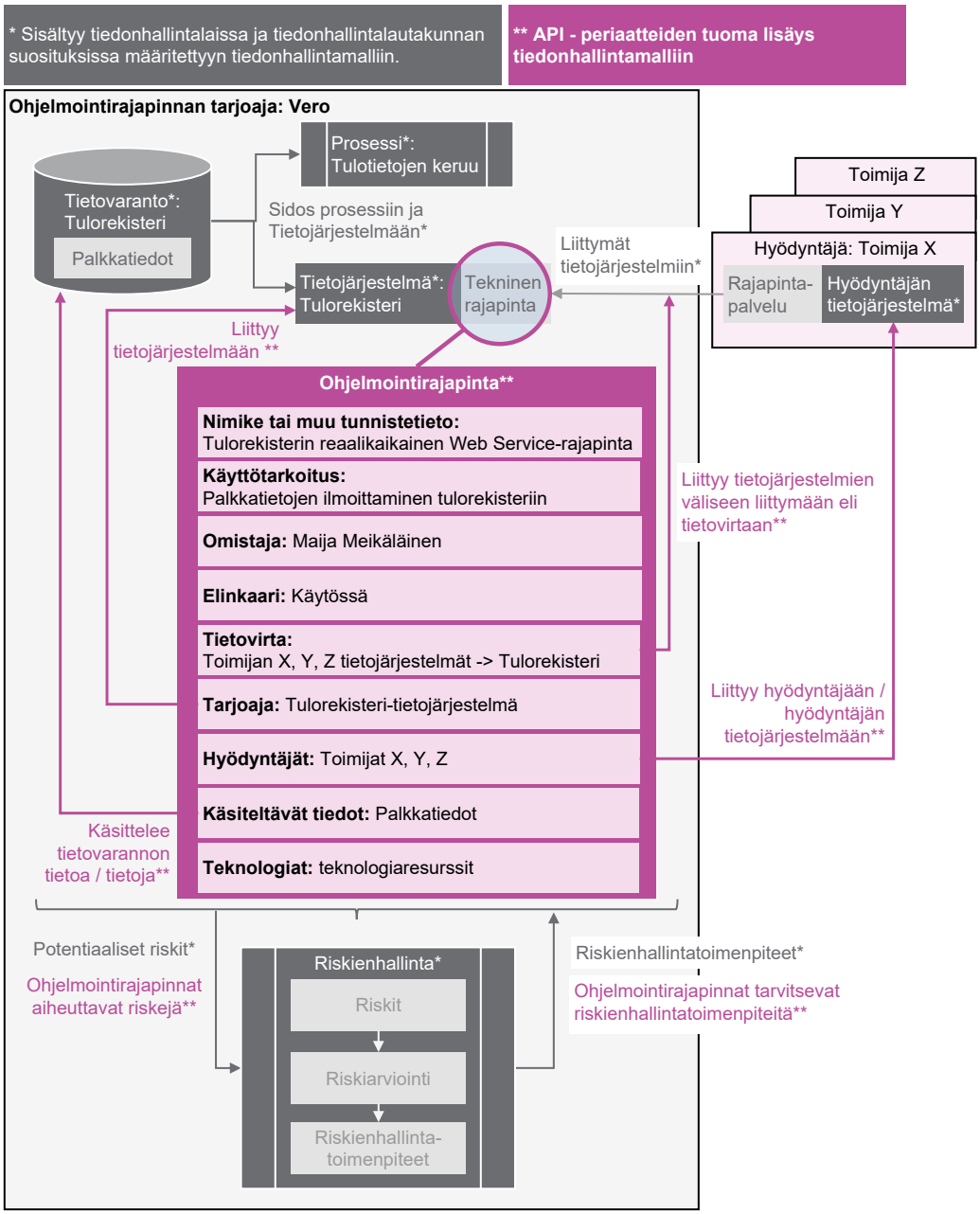
Kuvat 7 ja 8 sisältävät esimerkit ohjelmointirajapintojen kuvauksesta ohjelmointirajapinnan tarjoajan ja hyödyntäjän näkökulmasta osana organisaation tiedonhallintamallia. Esimerkissä on huomioitu Tiedonhallintalakiin[56] perustuva Tiedonhallintalautakunnan suositus[57] tiedonhallintamallista. Kuvat ovat kuvitteellisia ja esimerkinomaisia, vaikka perustuvatkin Verohallinnon todellisuudessa tarjoamaan tulorekisterirajapintaan[58], jonka avulla muut toimijat voivat ilmoittaa automaattisesti palkkatietojaan Verohallinnolle.

56 Tiedonhallintalain 5§ (Tiedonhallintalaki 906/2019, 2019)

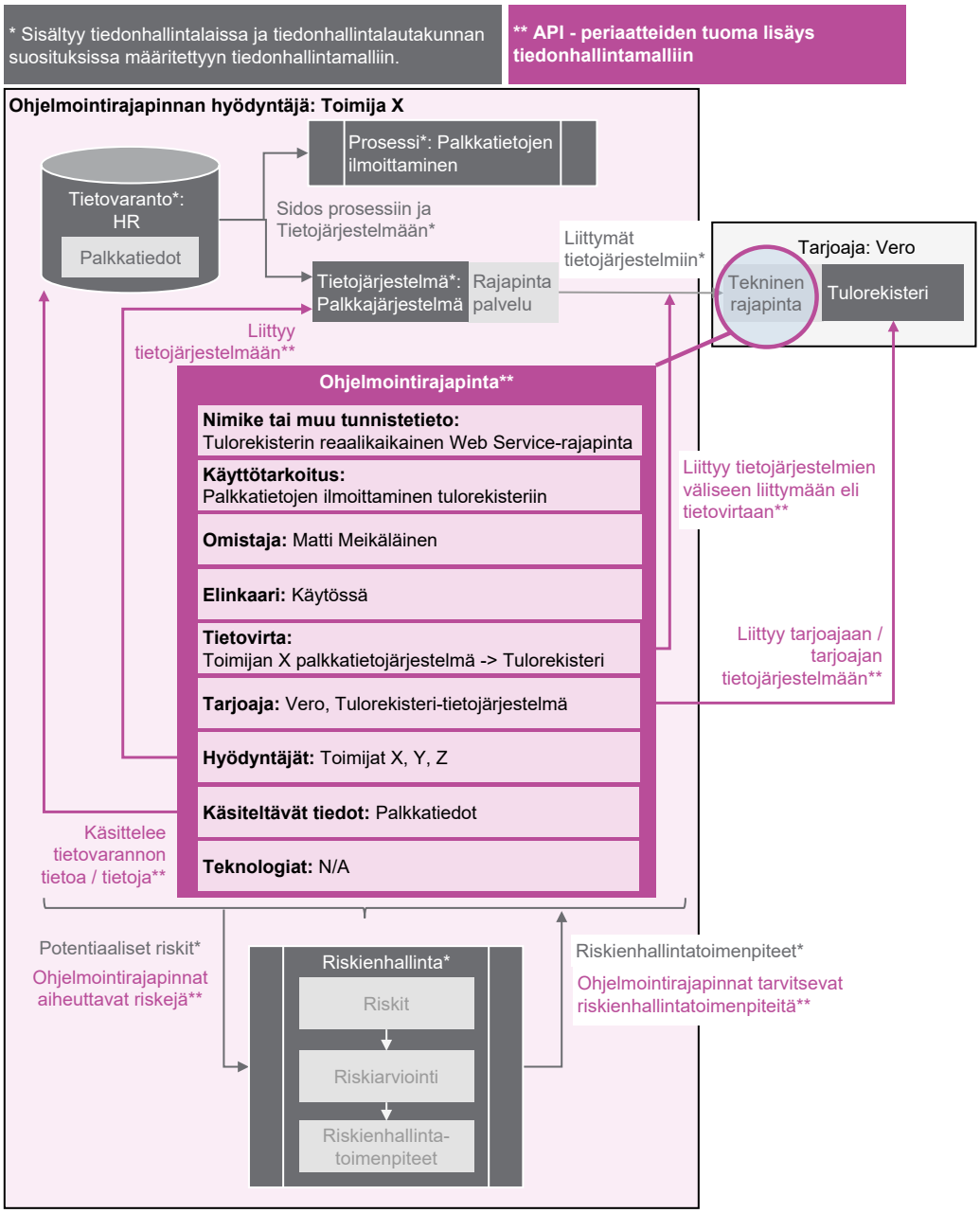
57 Suositus tiedonhallintamallista (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:29)

58 Tulorekisterin tekninen rajapinta (Verohallinto, 2021a)

Kuva 7. Suositus ohjelmointirajapintojen kuvauksesta osana tiedonhallintamallia ohjelmointirajapinnan tarjoajan näkökulmasta



Kuva 8. Suositus ohjelmointirajapintojen kuvauksesta osana tiedonhallintamallia ohjelmointirajapinnan hyödyntäjän näkökulmasta



TUOTOKSET

- Ohjelmointirajapintojen kuvaukset esimerkiksi osana tiedonhallintamallia.

HYÖDYT

- Ohjelmointirajapinnan eri arkkitehtuurinäkökulmien kuvaaminen auttaa organisaatiota ymmärtämään ohjelmointirajapintojen merkityksen omalle toiminnalleen, tietoaineistoilleen, tietojärjestelmilleen, tietovirroilleen ja käytettäville teknologioilleen.
- Ohjelmointirajapinnan linkittäminen tietoon, tietoaineistoon tai tietoryhmään on erityisen tärkeää, sillä ohjelmointirajapinnan käsittelemän tiedon luokitus auttaa organisaatiota ymmärtämään ohjelmointirajapinnan aiheuttamat riskit ja tarvittavat tietoturvatoimenpiteet paremmin.
- Hallittu ohjelmointirajapintakokonaisuus edistää ohjelmointirajapintojen uudelleenkäytettävyyttä, yhteentoimivuutta sekä tietoturvaa ja tietosuojaa.

TUKIMATERIAALI

Tutustu myös seuraaviin materiaaleihin, joista voit saada apua kokonaisarkkitehtuurin ja tiedonhallintamallin ymmärtämiseen ja kuvaamiseen:

- Tiedonhallintalautakunnan suositus tiedonhallintamallista[59].
- eOppivan koulutus: Johdanto kokonaisarkkitehtuuriin[60].
- eOppivan koulutus: Kokonaisarkkitehtuurin mallintaminen[61].

59 Tiedonhallintalautakunnan suositus tiedonhallintamallista (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:29)

60 Johdanto kokonaisarkkitehtuuriin (eOppiva, 2021a)

61 Kokonaisarkkitehtuurin mallintaminen (eOppiva, 2021b)

Periaate 2.4 Tunnista ja hallitse ohjelmointirajapintoihin liittyvät riskit

Määritä ja ota käyttöön menetelmä ohjelmointirajapintoihin liittyvien riskien ja uhkien tunnistamiseen sekä riskienhallintatoimenpiteiden toteuttamiseen ja seurantaan. Sisällytä riskienhallintatoimenpiteet osaksi ohjelmointirajapintojen toiminnallisia ja ei-toiminnallisia vaatimuksia.

Hyödynnä riskienhallintaan Digitaalisen turvallisuuden johtoryhmän VAHTI:n laatimaa riskienhallintaohjetta[62] ja organisaatiossasi jo olemassa olevia riskienhallinnan prosesseja. Riskienhallinnan prosessi voi edetä esimerkiksi seuraavasti:

- Valitse riskienhallinnan kohteena oleva ohjelmointirajapinta tai ohjelmointirajapintojen muodostama palvelukokonaisuus.
- Tunnista ohjelmointirajapintojen käsittelemät tiedot ja toiminnallisuudet, niiden luokittelu ja hallinnoijat.
- Tunnista ohjelmointirajapintojen kriittisyys toiminnan kannalta ja siihen liittyvät tekijät, kuten jatkuvuuteen ja palautumiseen liittyvät reunaehdot. Tunnista myös ohjelmointirajapinnan toimintaan liittyvät riippuvuudet ja niistä mahdollisesti aiheutuvat kerrannaisvaikutukset.
- Tunnista ohjelmointirajapintaan ja sen käsittelemään tietoon tai toiminnallisuuteen liittyvät uhat ja riskit. Huomioi myös palvelutuotantoon ja palvelutasoihin liittyvät riskit.
- Priorisoi tunnistetut riskit ja määrittele niille hallintatoimenpiteet.
- Määrittele riskienhallintatoimenpiteiden toteutus- ja seurantavastuut sekä muut mahdolliset jatkotoimenpiteet, kuten ohjelmointirajapintojen jatkuvuus- ja toipumissuunnitelmien teko tai päivitys.

Huomioi lakisääteiset vaatimukset tietojen käsittelylle tietoturvatoimenpiteiden suunnittelussa. Turvallisuusluokitellun tiedon käsittelyssä noudatetaan turvallisuusluokiteltavien asiakirjojen käsittelyohjeita[63], luottamukselliset viestintätiedot suojataan sähköisen viestinnän palveluista annetun lain[64] mukaisesti ja henkilötiedot suojataan ohjelmointirajapinnoissa tietosuoja-asetuksen[65] ja -lain[66] mukaisesti.

62 VAHTI riskienhallintaohje (Digi- ja väestötietovirasto, 2021a)

63 Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:19)

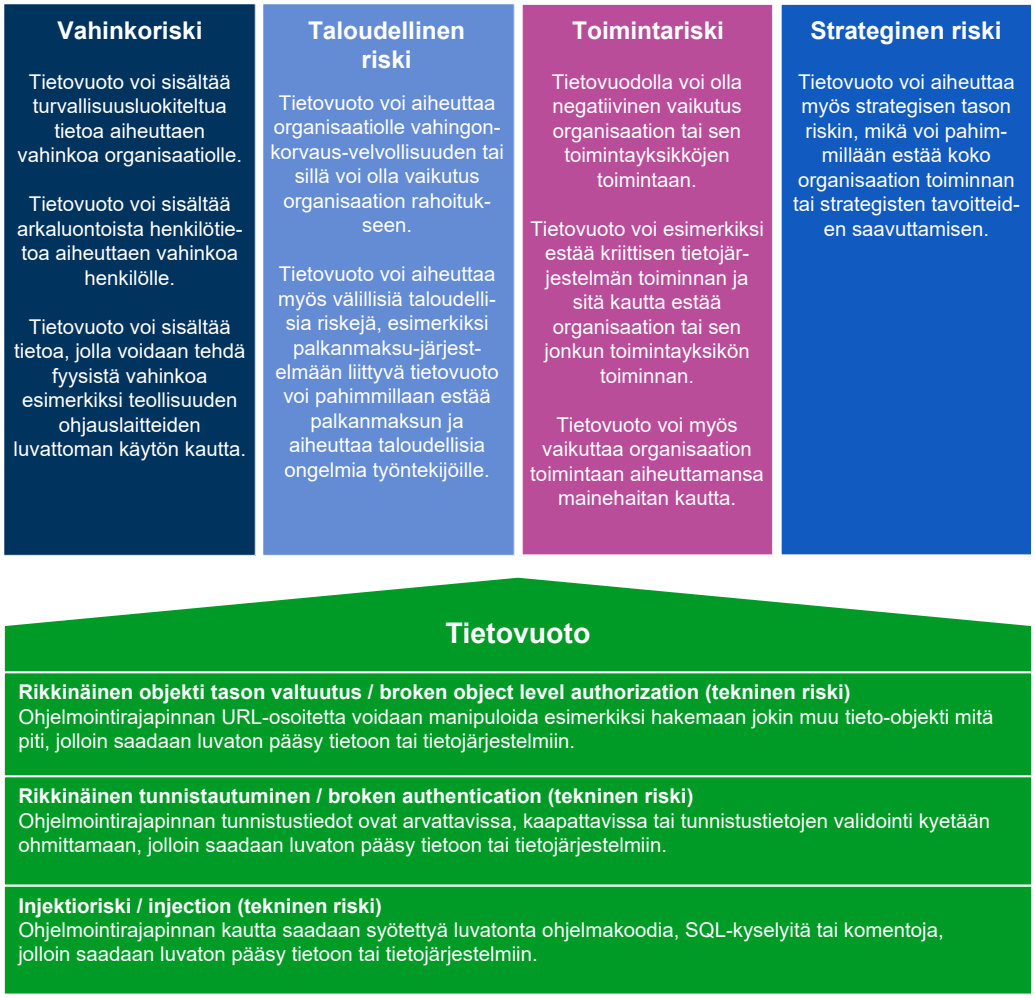
64 Laki sähköisen viestinnän palveluista (Laki sähköisen viestinnän palveluista 7.11.2014/917, 2014), tutustu myös Kyberturvallisuuskeskuksen Luottamuksellinen viestintä -sivustoon (Kyberturvallisuuskeskus, 2021b)

65 Yleinen tietosuoja-asetus (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 2016/679)

66 Tietosuojalaki (Tietosuojalaki , 5.12.2018/1050)

Huomioi myös, että ohjelmointirajapintoihin liittyvillä riskeillä voi olla heijastusvaikutuksia muihin tunnistettuihin riskeihin organisaation eri riskienhallinnan tasolla. Kuvassa 9 on esimerkki siitä, miten kolme eri OWASP API Top 10 -riskilistalla[67] olevaa riskiä voi aiheuttaa tietovuodon, jolloin luonteeltaan tekninen riski voi eskaloitua vahinkoriskiksi, taloudelliseksi riskiksi, toimintariskiksi tai strategiseksi riskiksi. Tämän vuoksi myös ohjelmointirajapintojen riskienhallinnassa tulisi ottaa huomioon tunnistettujen uhkien ja riskien vaikutus organisaation toimintaan.

Kuva 9. Esimerkki ohjelmointirajapintojen aiheuttamasta riskistä



67 OWASP API Top 10 Security Risks (OWASP, 2019)

TUOTOKSET

- Riskirekisteri, sisältäen ohjelmointirajapintojen aiheuttamat riskit.
- Riskienhallintatoimenpiteet ohjelmointirajapinnoille sisältäen myös jatkuvuuteen ja toipumiseen liittyvät toimenpiteet.

HYÖDYT

- Ohjelmointirajapintoihin kohdistuvien riskien tunnistamisen ja hallinnan avulla organisaatio voi minimoida ohjelmointirajapintojen toiminnalle tai toiminnan jatkuvuudelle aiheutuvia riskejä ja haittoja.
- Riskienhallinta edistää ohjelmointirajapintojen tietoturvaa ja tietosuojaa.

TUKIMATERIAALI

Tutustu seuraaviin aineistoihin, joista voit saada apua ohjelmointirajapintoihin liittyvien riskien tunnistamiseen ja riskien hallintaan:

- Tiedonhallintalautakunnan suosituskokoelma tiettyjen turvallisuussäännösten soveltamisesta[68], joka sisältää kuvauksen tietoriskienhallinnasta.
- VAHTI riskienhallintaohje[69].
- Liitteen 1 esimerkki ohjelmointirajapintojen riskienhallinnasta tietoriskianalyysin avulla.
- OWASP API Security Top 10 -lista[70], joka sisältää ohjelmointirajapintoihin yleisimmin kohdistuvat riskit ja niiden hallintatoimenpiteet.
- Kyberturvallisuuskeskuksen Turvallinen tuotekehitys – kohti hyväksyntää opas[71], joka sisältää parhaita käytäntöjä haavoittuvuuksien ja muiden yleisimpien ongelmien välttämisestä ohjelmistotuotannossa.
- Zero Trust Architecture (englanniksi)[72], joka sisältää kuvauksen nollaluottamusmallista.

68 Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:65)

69 VAHTI riskienhallintaohje (Digi- ja väestötietovirasto, 2021a)

70 OWASP API Security Top 10 2019 The ten most critical API security risks (OWASP, 2019)

71 Kyberturvallisuuskeskuksen Turvallinen tuotekehitys – kohti hyväksyntää opas (Kyberturvallisuuskeskus, 2020)

72 Zero Trust Architecture (NIST, 2020)

3.3 Operatiivinen taso

Kuva 10. Operatiivisen tason periaatteet

Periaate 3.1 Kehitä ohjelmointirajapinnat avoimilla ja teknologiariippumattomilla standardeilla ja protokollilla

Määritä ohjelmointirajapintojen kehittämisessä tarvittavat standardit, protokollat ja teknologiat. Ohjelmointirajapintojen kehittämiseen tarvitaan esimerkiksi:

- **Tiedonsiirtoprotokolla**, joka määrittää millä tavalla tietoa voidaan tuoda tai hakea ohjelmointirajapinnasta. **Suositeltavaa on hyödyntää ohjelmointirajapinnoissa ensisijaisesti avoimia, yleisesti käytössä olevia ja teknologiariippumattomia web-pohjaisia tiedonsiirtoprotokollia.**
- **Tiedostomuoto**, joka määrittää missä muodossa ohjelmointirajapinnan käsittelemä tieto kuvataan. Tiedostomuodon tulee olla koneluettavaa. Tiedostomuoto voi perustua esimerkiksi johonkin avoimeen tai vaikkapa toimialakohtaiseen standardiin tai notaatioon.
- **Tietoturvaan liittyvät protokollat ja menetelmät**, joiden avulla voidaan toteuttaa mm. salausta ja pääsynhallintaa.
- **Toimialakohtaiset standardit**, jotka määrittävät jollain tietyllä toimialalla kansallisesti tai kansainvälisesti yhteisesti käytössä olevat tavat.

Määritä mitä tiedonsiirtoprotokollia, tiedostomuotoja, tiedon sisältöön tai tietoturvaan liittyviä standardeja, protokollia tai menetelmiä organisaatiossasi käytetään. **Suosi valinnoissa avoimia, nykyaikaisia ja yleisesti käytössä olevia teknologiariippumattomia standardeja ja protokollia.** Huomioi määrityksissä sekä sisäisten (sisäinen API) että ulkoisten (kumppani API, julkinen API) ohjelmointirajapintojen kehittäminen.

Huomioi määrityksissä toimialakohtaiset standardit ja ohjeistukset sekä lakisääteiset tai muut velvoitteet, jotka asettavat vaatimuksia tai rajauksia käytettäville standardeille tai protokollille. Esimerkiksi laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista[73] asettaa velvoitteen käyttää tietyissä tilanteissa Suomi.fi -palveluväylää[74]. Velvoitteen piirissä olevat ohjelmointirajapinnat tulee kehittää Suomi.fi -palveluväylän tukemilla standardeilla tai protokollilla.

Huomioi myös, että käytettävien tietoturvaprotokollien tai menetelmien tulee mahdollistaa riskienhallinnan määrittämien tietoturvatoimenpiteiden toteuttaminen eli ne on valittava määritettyjen tietoturvatoimenpiteiden perusteella. Tietoturvatoimenpiteet määräytyvät esimerkiksi ohjelmointirajapinnan käsittelemän tiedon turvallisuusluokituksen perusteella.

Ota valitut standardit, protokollat ja teknologiat käyttöön ohjelmointirajapintojen kehittämisessä.

---

73 Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista 3§, 5§ (Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista, 571/2016)

74 Suomi.fi-palveluväylä (Digi- ja väestötietovirasto, 2021b)

TUOTOKSET

- Ohjeistus ohjelmointirajapintojen kehittämisessä käytettävistä standardeista, protokollista ja teknologioista.
- Valituilla standardeilla ja protokollilla kehitetyt ohjelmointirajapinnat.

HYÖDYT

- Ohjelmointirajapintojen kehittämistyö tehostuu, ylläpito helpottuu ja erilaisen osaamisen tarve vähenee, kun keskitetään osaamista valittuihin standardeihin, protokolliin ja teknologioihin.
- Avointen, yleisesti käytössä olevien standardien, protokollien ja teknologioiden hyödyntäminen edistää ohjelmointirajapintojen uudelleenkäytettävyyttä ja teknistä yhteentoimivuutta.
- Osaamisen keskittäminen valittuihin standardeihin, protokolliin ja teknologioihin edistää ohjelmointirajapintojen laatua.

TUKIMATERIAALI

Esimerkkejä ja lisätietoa tiedonsiirtoprotokollista:

- Web-pohjaisissa ohjelmointirajapinnoissa hyödynnetään yleensä http-pohjaista tiedonsiirtoprotokollaa tai arkkitehtuurimallia, kuten SOAP[75], REST (Representational State Transfer)[76] tai GraphQL[77]. Web-pohjaisia rajapintoja voidaan hyödyntää sekä sisäisissä että ulkoisissa rajapinnoissa ja niihin saadaan toteutettua laajasti erilaisia tietoturvakontrolleja. Web-pohjaiset rajapinnat mahdollistavat tietojen ja toiminnallisuuksien reaaliaikaisen hyödyntämisen synkronisesti tai asynkronisesti[78].Tiedot ja toiminnallisuudet on suositeltavaa tarjota web-pohjaisten rajapintojen kautta, jos mahdollista ja käyttötarkoituksen mukaista. Synkronisuus / asynkronisuus tulee määrittää ohjelmointirajapinnoille asetettujen tarpeiden ja vaatimusten perusteella.
- Tiedostopohjaisissa ohjelmointirajapinnoissa hyödynnetään yleensä jotain tiedostopohjaista protokollaa kuten FTP, SFTP tai FTPS. Myös http-pohjaisia protokollia voidaan hyödyntää tiedostojen tarjoamiseen tai vastaanottamiseen. Tiedostopohjaisia ohjelmointirajapintoja voidaan hyödyntää sekä sisäisissä että ulkoisissa rajapinnoissa. Ulkoisissa rajapinnoissa on huolehdittava riittävien tietoturvakontrollien toteuttamisesta. Tiedostopohjaiset rajapinnat ovat hyviä silloin, kun tietoa tai toiminnallisuuksia ei tarvita reaaliaikaisesti tai siirrettävät tiedot ovat tiedostomuotoisia, esimerkiksi kuvia, videoita tai vaikkapa Excel-taulukoita.
- Tietokantapohjaisissa ohjelmointirajapinnoissa hyödynnetään yleensä jotain tietokantapohjaista protokollaa, kuten ODBC tai JDBC[79], jonka avulla mahdollistetaan toisen tietojärjestelmän, sovelluksen tai ohjelmiston yhteyden avaaminen tietokantaan ja operaatioiden suorittaminen tietokantaa vasten. Tietokantapohjaisia ohjelmointirajapintoja ei suositella käytettävän kuin organisaation sisäisesti. Esimerkiksi tietokantapohjaista rajapintaa voidaan hyödyntää tietojen keräämisessä ETL-integraatiolla[80] keskitettyyn tietovarastoon. Mikäli on tarve tarjota jonkin tietovarannon tietoja muille toimijoille, tulee kehittää esimerkiksi web-pohjainen ohjelmointirajapinta tietovarannon ja toisen toimijan väliin.

75 XML Soap (W3Schools, 2021e)
76 RESTFul Web Services (W3Schools, 2021b)
77 A query language for your API (GraphQL Foundation, 2021)
78 Synchronous/asynchronous API (TechTarget, 2017)
79 What is the difference between ODBC and JDBC (Sharma, et al., 2019)
80 ETL (Extract, Transform, Load) (IBM, 2020)

Esimerkkejä ja lisätietoa tiedostomuodoista:

- Web-pohjaisissa rajapinnoissa hyödynnetään yleensä XML:ää[81] tai JSON:ia[82]. XML sanomat voidaan kuvata XML skeeman[83] avulla ja JSON sanomat JSON Skeeman[84] avulla.
- Tiedostopohjaisissa rajapinnoissa tiedostomuoto voi oikeastaan olla mitä vain, esimerkiksi kuvatiedosto (.jpg, .gif, .png), videotiedosto (.mp4, .avi) tai taulukko (.xslx, .csv).
- Tietokantapohjaisissa rajapinnoissa tiedostomuoto on yleensä tietokannan määrittämä rakenne, joka voi perustua näkymään, tauluun, proceduuriin tai muuhun kantaskriptiin.

Esimerkkejä ja lisätietoa tietoturvaan liittyvistä protokollista ja menetelmistä:

- Ohjelmointirajapinnoissa tiedon ja tietoliikenteen salaus toteutetaan yleisimmin suojatun HTTPS[85]-tiedonsiirto- ja TLS[86]-salausprotokollan avulla. Salauksen lisäksi esimerkiksi kumppaneille tarkoitetuissa ohjelmointirajapinnoissa voidaan hyödyntää myös VPN-teknologioita (Virtual Private Network) tunneloidun yhteyden muodostamiseksi palvelun tarjoajan ja hyödyntäjän välille. Turvallisuusluokiteltavia tietoja käsiteltäessä salauksen tulee noudattaa kyberturvallisuuskeskuksen kryptografisia vahvuusvaatimuksia[87].
- Ohjelmointirajapinnoissa voidaan hyödyntää esimerkiksi http(s)-protokollan mahdollistamia Basic- tai Bearer-autentikaatioita, API-avaimeen perustuvaa autentikaatiota, OAuth-protokollaa tai siitä johdettuja muunnoksia tai varmenteita. Tunnistusmekanismi on valittava riskiarvioinnin avulla.
- Tutustu myös Kyberturvallisuuskeskuksen ohjeistukseen sähköisestä tunnistamisesta[88] ja Digi- ja väestötietoviraston tunnistus- ja valtuudet-palveluihin[89].

81 XML Tutorial (W3Schools, 2021f)
82 JSON - Introduction (W3Schools, 2021a)
83 XML Schema Tutorial (W3Schools, 2021d)
84 JSON Schema (JSON Schema, 2021)
85 REST Security Cheat Sheet, HTTPS (OWASP Cheat Sheet Series, 2021a)
86 Transport Layer Protection Cheat Sheet (OWASP Cheat Sheet Series, 2021b)
87 Kyberturvallisuuskeskuksen vahvuusvaatimukset (Kyberturvallisuuskeskus, 2021a)
88 Kyberturvallisuuskeskus, sähköinen tunnistaminen (Kyberturvallisuuskeskus, 2021c)
89 Tunnistus- ja valtuudet palvelut (Digi- ja väestötietovirasto, 2021c), (Digi- ja väestötietovirasto, 2021d)

Esimerkkejä toimialakohtaisista standardeista ja ohjeistuksista:

- Paikkatietoalan standardit ja suositukset[90].
- Rajapintakartta Sosiaali- ja terveydenhuollon integraatioita ja tietojärjestelmiä varten[91].
- Suomen Standardisoimisliitto SFS Ry:n standardisoimisryhmien laatimat kansalliset ja kansainväliset standardit[92].
- Kirjastojen, arkistojen ja museoiden (KAM-sektorin) FINNA-hakuliittymässä, pitkäaikaissäilytyksen Kulttuuriaineisto-PAS -palvelussa sekä muissa yhteisissä järjestelmissä kuten FINTO-ontologiapalvelussa sovellettavat standardit[93].
- Kansallisten pitkäaikaissäilytyspalveluiden (PAS-palveluiden) säilytys- ja siirtokelpoiset tiedostomuodot[94]

Periaate 3.2 Kuvaa ohjelmointirajapintojen käsittelemät tiedot yhteisten ja yleisten tietomallien mukaisesti

Määritä ja ota käyttöön ohjelmointirajapintojen käsittelemän tiedon kuvaamisessa tarvittavat tietomallit ja metatiedot. Hyödynnä yleisiä tai yhteisiä sanastoja, koodistoja, tietomalleja, tietorakenteita, luokitteluja ja laatukriteerejä[95]. Tiedonhallintalautakunnan suosituksen mukaan 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 noudatettava lakia. Laissa säädetyt käsitteet sitovat niiden käyttöä viranomaisten toiminnassa[96].

90 Paikkatietoalan standardit ja suositukset (Maanmittauslaitos, 2021a)

91 Rajapintakartta (HL7 Finland, 2021)

92 Standardisointiryhmät (Suomen standardisoimisliitto SFS Ry, 2021a)

93 Digime-standardisalkku (Digime-tietoarkkitehtuuriryhmä, 2021)

94 Säilytys- ja siirtokelpoiset tiedostomuodot (CSC – Tieteen tietotekniikan keskus Oy, 2021)

95 Tiedonhallintalautakunnan suositus teknisistä rajapinnoista ja katseluyhteyksistä, s 11 (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:21)

96 Lisätietoja Tiedonhallintalautakunnan suosituksesta teknisistä rajapinnoista ja katseluyhteyksistä (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:21)

TUOTOKSET

- Ohjeistus ohjelmointirajapintojen tietojen kuvaamisessa käytettävistä yhteisistä ja yleisistä tietomalleista ja metatietomalleista.
- Ohjelmointirajapintojen käsittelemät tiedot on mallinnettu yhteisten ja yleisten tietomallien mukaisesti.

HYÖDYT

- Ohjelmointirajapintojen käsittelemien tietojen mallinnus tehostuu ja helpottuu, kun voidaan hyödyntää jo olemassa olevia tietomalleja, metatietomalleja, koodistoja ja sanastoja eikä tarvitse keksiä näitä joka kerta uudelleen.
- Yhteiset tietomallit, metatietomallit, koodistot ja sanastot edistävät ohjelmointirajapintojen uudelleenkäytettävyyttä, semanttista yhteentoimivuutta ja laatua.

TUKIMATERIAALI

Tukimateriaaleja, joista voit saada apua yhteisten ja yleisten tietomallien, metatietomallien, sanastojen ja koodistojen tunnistamisessa:

- Yhteentoimivuusalusta ja yhteentoimivuusmenetelmä[97], joka sisältää työkalut yhteentoimivien tietosisältöjen määrittelyyn.
- Tilastokeskuksen tiedon laatukriteerit ja mittarit[98], joka sisältää ohjeita tietoaineistojen laadun kuvaamiseen ja arvioimiseen.
- Kuntaliiton julkaisema Yhteentoimivuus kunnissa -video[99], joka sisältää lisätietoa yhteentoimivuudesta kunnissa.
- Finto.fi[100], joka sisältää keskitetyn palvelun eri alojen yhteentoimiville sanastoille, ontologioille ja luokituksille.

97 Yhteentoimivuusalusta ja yhteentoimivuusmenetelmä (Digi- ja väestötietovirasto, 2021e)

98 Tietoaineistojen laatukriteerit ja mittarit (Tilastokeskus, 2021)

99 Yhteentoimivuus kunnissa – video (Kuntaliitto, 2021)

100 Finto.fi - keskitetty palvelu eri alojen yhteentoimiville sanastoille, ontologioille ja luokituksille (Kansalliskirjasto, 2021)

Periaate 3.3 Turvaa, testaa, versioi, dokumentoi ja julkaise ohjelmointirajapinnat

Turvaa ohjelmointirajapinta. Toteuta riskienhallinnassa määritetyt tietoturvatoimenpiteet.

Testaa ohjelmointirajapinta. Määritä ohjelmointirajapinnan testausta varten testitapaukset, joiden avulla voidaan testata toiminnalliset ja ei-toiminnalliset vaatimukset kuten käytettävyys, vikasietoisuus, tietoturva ja suorituskyky. Huomioi testauksen eri vaiheet: yksikkö-, integraatio-, järjestelmä- ja hyväksymistestaus sekä regressiotestaus. Hyödynnä testauksessa testausautomaatiota mahdollisuuksien mukaan. **Julkaise ohjelmointirajapinnasta myös maksuton testiversio ja testausohjeet hyödyntäjien testausta varten.**

Versioi ohjelmointirajapinta. Huomioi versioinnissa sekä taaksepäin yhteensopivien että yhteensopimattomien muutosten ja korjausten julkaisu. Huomioi myös useampien rajapintaversioiden samanaikainen tukeminen mahdollisten tarpeiden mukaisesti.

Dokumentoi ohjelmointirajapinta. Sisällytä dokumentointiin:

- Käyttötarkoitus: Mihin ohjelmointirajapinta ja sen tarjoamat tiedot tai toiminnallisuudet on tarkoitettu? Mitä rajoitteita tai rajoituksia hyödyntämiselle on?
- Lisensointi: Miten ohjelmointirajapinta ja sen tarjoamat tiedot tai toiminnallisuudet on lisensoitu?
- Sijainti: Missä ohjelmointirajapinta sijaitsee?
- Ohjelmointirajapinnan palvelutaso tai -lupaus: Millainen palvelutaso tai palvelulupaus ohjelmointirajapinnalla on? Kerro jos palvelutasoa tai lupausta ei ole, esimerkiksi jos kyseessä on kokeiluasteella oleva rajapinta.
- Testaus- ja käyttöönotto-ohjeet: Miten ohjelmointirajapinnan hyödyntäjät voivat testata rajapintaa? Miten hyödyntäjät voivat ottaa rajapinnan käyttöön?
- Ohjelmointirajapinnan tarjoamat operaatiot tai metodit: Mitä operaatioita tai metodeja rajapinta tarjoaa? Mikä on yksittäisen operaation tai metodin käyttötarkoitus?
- Ohjelmointirajapinnan operaatioiden tai metodien pyyntö (request)- ja vastaussanomat (response): Millainen rakenne pyyntö- ja vastaussanomissa on? Mitä kenttiä ne sisältävät? Mitkä ovat kenttien tietotyypit ja mahdolliset rajoitteet tietosisällöille? Millaisia arvoja kentät sisältävät? Mitä arvot tarkoittavat? Huomioi erityisesti mahdollisesti käytettyjen viiteavainten tai koodistoarvojen merkityksen avaaminen.
- Ohjelmointirajapinnan operaatioiden tai metodien palauttamat mahdolliset virhekoodit ja niiden selitteet: Mitä virhekoodeja ohjelmointirajapinta voi palauttaa? Mitä virhekoodit tarkoittavat? Miten hyödyntäjän pitäisi mihinkin virhekoodiin reagoida?

- Ohjelmointirajapinnasta vastaavan toimijan tai tahon yhteystiedot: Mihin ja miten hyödyntäjät voivat olla yhteydessä, jos heillä on ohjelmointirajapintaan liittyviä kysymyksiä, ongelmia tai lisätarpeita?

Hyödynnä dokumentoinnissa mahdollisuuksien mukaan välineitä, jotka generoivat ainakin osan dokumentaatiosta automaattisesti. Sisällytä dokumentaatiota esimerkiksi osaksi ohjelmointirajapinnan metatietoja. Ulkoisten sidosryhmien, kuten palvelutoimittajien, tuottamien ohjelmointirajapintojen dokumentaatioiden toteuttaminen ja ylläpito tulee velvoittaa kumppanisopimuksissa.

Julkaise ohjelmointirajapinta dokumentaatioineen käyttötarkoituksensa mukaisessa julkaisukanavassa ja rajapintakatalogissa. Julkaisukanava riippuu ohjelmointirajapinnan tyypistä (sisäinen, kumppani vai julkinen API), ohjelmointirajapinnan hyödyntäjistä ja ohjelmointirajapinnan käsittelemän tiedon luokittelusta. Huomioi myös, että lainsäädännöstä voi tulla velvoitteita jonkin julkaisukanavan käyttöön. Esimerkiksi laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista[101] asettaa velvoitteen käyttää tietyissä tilanteissa Suomi.fi -palveluväylää[102].

TUOTOKSET

- Tietoturvakontrollien toteutus.
- Testitapaukset, testaussuunnitelmat ja testiraportit.
- Testirajapinta ja testausohjeet.
- Versiointikäytännöt.
- Rajapintojen dokumentaatiot.
- Rajapintojen tiedot rajapintakatalogissa.
- Toiminnalliset ja ei-toiminnalliset vaatimukset täyttävä, tietoturvallinen, versioitu ja dokumentoitu ohjelmointirajapinta julkaistuna oikeaan julkaisukanavaan.

101 Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista 3§, 5§ (Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista, 571/2016)

102 Suomi.fi-palveluväylä (Digi- ja väestötietovirasto, 2021b)

HYÖDYT

- Turvaamalla ja testaamalla ohjelmointirajapinnat organisaatio kykenee varmistamaan, että ohjelmointirajapinnat toimivat oikein eli täyttävät niille asetetut toiminnalliset ja ei-toiminnalliset vaatimukset.
- Versioinnilla, dokumentoinnilla ja oikeanlaisella julkaisukanavalla organisaatio kykenee varmistamaan, että kehitetyt ohjelmointirajapinnat ovat käyttöönotettavissa ja ylläpidettävissä.
- Toimivat ja ylläpidetyt ohjelmointirajapinnat edistävät asiakaslähtöisyyttä ja yhteistyötä, uudelleenkäytettävyyttä, yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä laatua.

TUKIMATERIAALI

Esimerkkejä hyvin dokumentoiduista rajapinnoista, joissa on myös mahdollistettu hyödyntäjien testaus:

- Traficom Avoin Data API[103].
- Vero API[104].

Testaukseen liittyviä lisämateriaaleja (kaikki englanniksi), joista voit saada apua ohjelmointirajapintojen testauksen suunnitteluun:

- API:en testausohje, sisältää myös esimerkkejä ohjelmointirajapintojen testauksessa käytettävistä työkalusta[105].
- Muut järjestelmätestausohjeet, kuten W3Schools:n Software Testing Tutorial Library[106] tai Software Testing Fundamentals[107].
- DevOps Instituten julkaisema DevOps testausohje[108], joka sisältää jatkuvan testauksen mallin.

103 Traficom Avoin Data API (Traficom, 2021)
104 Vero API (Verohallinto, 2021b)
105 A Comprehensive API Testing Guide (Software Testing Materials, 2020)
106 Software Testing Tutorial Library (W3Schools, 2021c)
107 Sotware Testing Fundamentals (Software Testing Fundamentals, 2021)
108 DevOps Testing (Hornbeek, 2021)

Versiointiin liittyviä lisämateriaaleja, joista voit saada apua versiointikäytäntöjen määrittämisessä:

- Semanttinen versiointi[109].

Dokumentointiin liittyviä lisämateriaaleja, joista voit saada apua dokumentointikäytäntöjen määrittämisessä:

- Tutustu Open API Initiativen Open API Specification[110] ja RAML[111] määrityksiin.
- Useissa API-hallintatyökaluissa on mukana automaattinen API:en dokumentointi, jota kannattaa hyödyntää. Esimerkkejä API-hallintatyökaluista löytyy mm. Gartnerin vertaisarviointisivuilta[112]. Myös erillisiä työkaluja löytyy, kuten Swagger UI[113].

Esimerkkejä julkisten ohjelmointirajapintojen julkaisukanavista:

- Palvelutietovaranto tai avoindata.fi[114].

Esimerkkejä kumppaneille tarkoitettujen ohjelmointirajapintojen julkaisukanavista:

- Suomi.fi -palveluväylä[115] lain määrittämän käyttövelvoitteen[116] mukaisesti.
- VIA-integraatioalusta Valtion organisaation väliseen tiedonvaihtoon[117].
- Turvallisuusluokiteltua tietoa käsittelevät ohjelmointirajapinnat julkaistaan ko. luokittelun vaatimusten mukaisessa yhdyskäytäväratkaisussa[118] ja niihin liittyvä dokumentaatio säilytetään ko. luokittelun vaatimusten mukaisessa tallennuspaikassa[119].
- Lisäksi voi olla toimiala- tai organisaatiokohtaisia julkaisukanavia.

109 Semantic Versioning 2.0.0 (Preston-Werner, 2021)

110 Open API Specification (Open API Initiative, 2021)

111 The simplest way to model APIs (RAML, 2021)

112 Full Life Cycle API Management Reviews and Ratings (Gartner, 2021)

113 Swagger UI (Swagger, 2021)

114 Palvelutietovaranto (Digi- ja väestötietovirasto 2022a), Avoindata.fi -palvelu (Digi- ja väestötietovirasto 2022b)

115 Suomi.fi-palveluväylä (Digi- ja väestötietovirasto, 2021b)

116 Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista 3§, 5§ (Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista, 571/2016)

117 Valtorin integraatiopalvelut (Valtori, 2021)

118 Yhdyskäytäväohje (Kyberturvallisuuskeskus, 2021)

119 Suositus turvallisuusluokiteltujen tietojen käsittelystä (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:19)

Esimerkkejä sisäisten ohjelmointirajapintojen julkaisukanavista:

- Sisäinen, organisaation itse määrittämä julkaisukanava. Julkaisukanava voi olla esimerkiksi jonkinlainen API-Gateway[120] tai muu tuote tai itse kehitetty ratkaisu, jonka kautta sisäiset API:t ovat löydettävissä ja hyödynnettävissä.

Periaate 3.4 Seuraa ohjelmointirajapinnoille asetettuja mittareita ja muita seurantakohteita

1. **Tunnista seurattavat mittarit ja muut seurantakohteet.** Mittareita tai muita seurantakohteita voidaan johtaa toiminnalle asetetuista tavoitteista sekä ohjelmointirajapinnoille asetetuista toiminnallisista tai ei-toiminnallisista vaatimuksista (katso periaate 1.2). Mittareita ja muita seurantakohteita voidaan määrittää ja seurata strategisen tason lisäksi myös taktisella ja operatiivisella tasolla. Seurantaa varten tunnistetuille mittareille ja muille seurantakohteille kannattaa määrittää sallitut raja- tai odotusarvot sekä seurantatiheys. Osaa mittareista tai muista seurantakohteista voi seurata reaaliaikaisesti ja jatkuvasti, osaa taas tietyin väliajoin, esimerkiksi viikoittain, kuukausittain tai vuosittain. On hyvä myös määrittää, miten reagoidaan, kun jokin raja- tai odotusarvo ylittyy tai alittuu. Esimerkiksi mitä pitäisi tehdä, jos ohjelmointirajapintaan kohdistuu raja-arvot ylittävä kuormitus tai jos jonkin ohjelmointirajapinnan käyttöaste jää odotuksia matalammaksi.
2. **Kerää seurantaa varten tarvittavat tiedot.** Tietoja voidaan kerätä esimerkiksi erilaisten lokien tai kyselyiden avulla. Mikäli seurantaa varten kerätään henkilötietoja, tulee huomioida tietosuoja-asetuksen[121] ja -lain[122] asettamat vaatimukset niiden käsittelylle. Mikäli seurantaa varten kerättävät tiedot ovat turvallisuusluokiteltavia, tulee niitä käsitellä turvallisuusluokiteltavien asiakirjojen käsittelyohjeiden[123] mukaisesti.
3. **Seuraa ja valvo mittareita ja muita seurantakohteita** sekä niille asetettuja raja-arvoja. Valvontaa voidaan tehdä esimerkiksi automaattisesti erilaisten valvonta- tai monitorointiratkaisuiden avulla tai manuaalisesti tietyin väliajoin generoitujen raporttien avulla. Useat valvontaratkaisut sisältävät

120 Full Life Cycle API Management Reviews and Ratings. (Gartner, 2021)

121 Yleinen tietosuoja-asetus (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 2016/679)

122 Tietosuojalaki (Tietosuojalaki , 5.12.2018/1050)

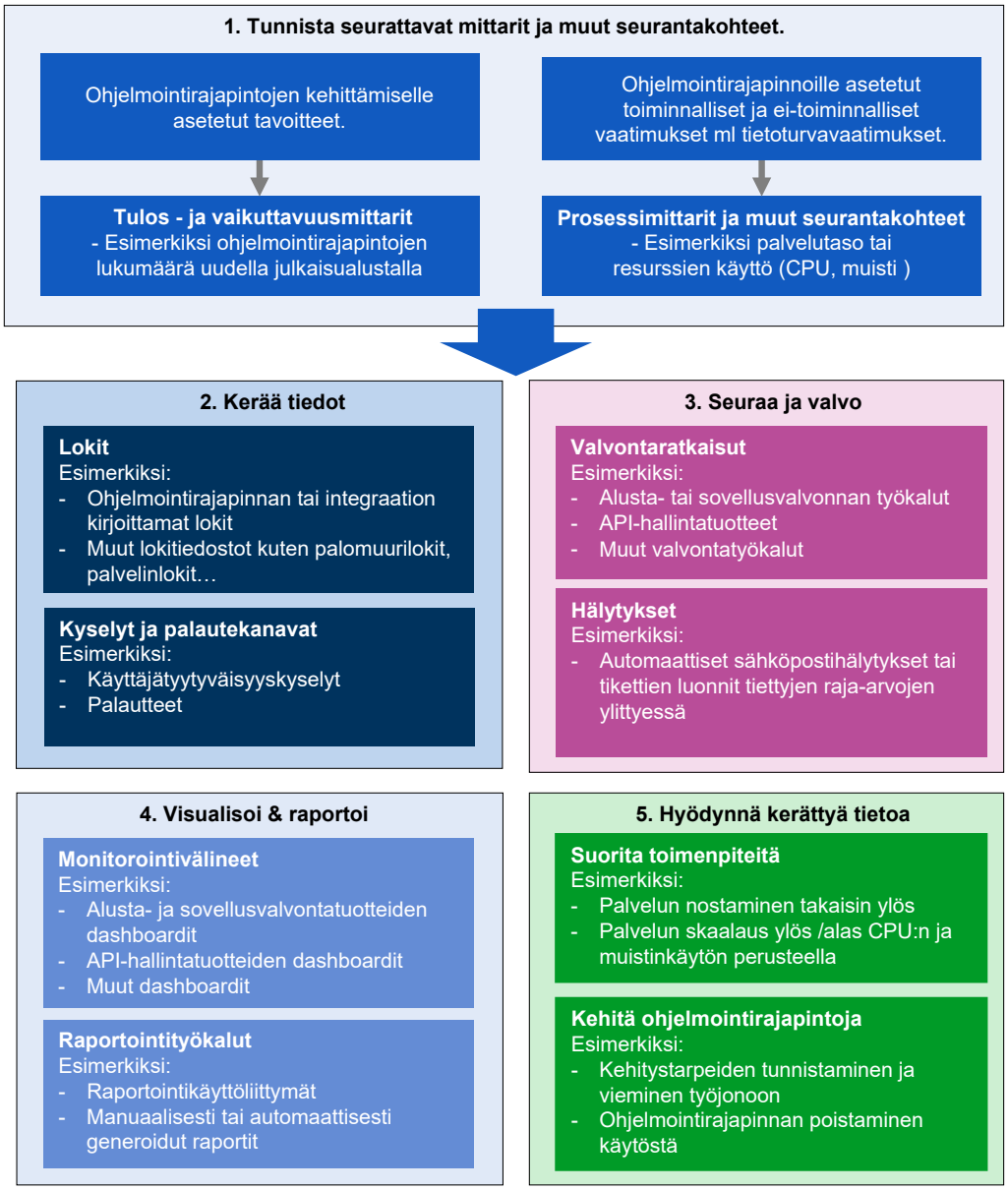
123 Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:19)

myös toiminnallisuuden, jonka avulla voit tehdä automaattisia hälytyksiä jonkin raja-arvon ylittyessä tai alittuessa.

4. **Visualisoi ja raportoi kerättyä tietoa.** Visualisointia voidaan tehdä esimerkiksi erilaisten monitorointi- tai valvontatyökalujen avulla tai hyödyntäen raportointiratkaisuja tai raportteja.
5. **Hyödynnä kerättyä tietoa tarvittavien toimenpiteiden tunnistamiseksi ja suorittamiseksi sekä ohjelmointirajapintojen kehittämiseksi tai käytöstä poistamiseksi.** Tiedon hyödyntämistä ja toimenpiteitä voidaan tehdä organisaation kaikilla tasoilla. Operatiivisella tasolla seurannan perusteella voidaan tunnistaa yksittäisiin ohjelmointirajapintoihin kohdistuvia kehitystarpeita tai kehityskohteita tai suorittaa tuotannon aikaisia toimenpiteitä, kuten ohjelmointirajapinnan nostaminen takaisin ylös sen ollessa alhaalla tai ohjelmointirajapinnan skaalaaminen kuormituksen perusteella. Hyödynnä toimenpiteissä mahdollisuuksien mukaan automatiikkaa. Taktisella tasolla seurannan perusteella voidaan tunnistaa yleisiä kehitystarpeita esimerkiksi ohjelmointirajapintojen toiminnallisuuksiin tai ei-toiminnallisuuksiin kuten käyttöön, käytettävyyteen, tietoturvaan tai kehittäjäkokemukseen liittyen. Strategisella tasolla kerättyä tietoa voidaan hyödyntää toiminnan kehittämiseen liittyvässä päätöksenteossa ja asetettujen tavoitteiden toteutumisen seuraamisessa.

Kuvassa 11 on visualisoitu ohjelmointirajapintojen seurantaan liittyvät tehtävät ja esimerkkejä eri seurantakohteista, kuten lokitietojen keräämisestä ja palautekanavista.

Kuva 11. Ohjelmointirajapintojen seuranta



TUOTOKSET

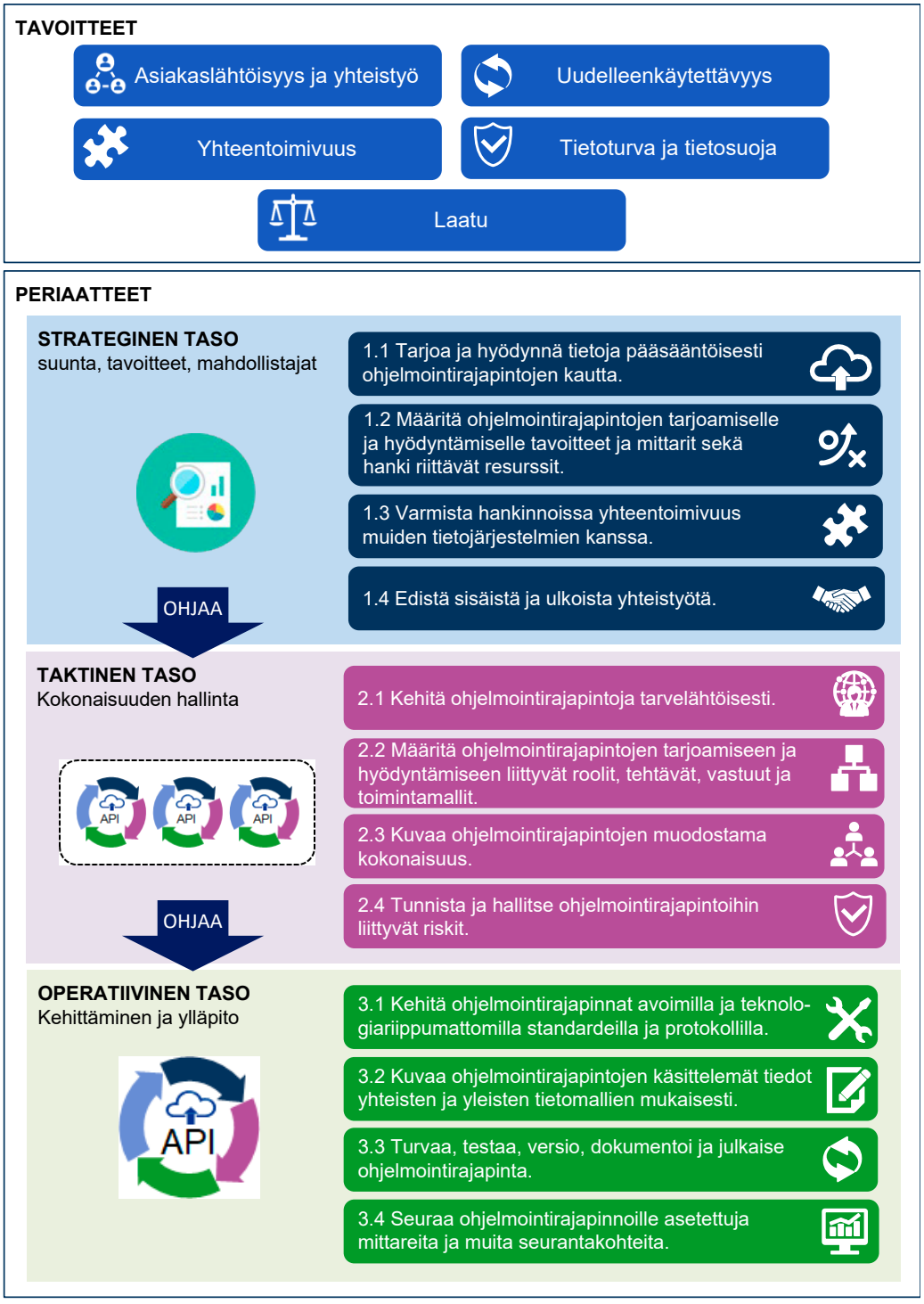
- Listaus seurattavista mittareista ja muista seurantakohteista raja-arvoineen.
- Ohjelmointirajapintojen ja integraatioiden lokitiedostot, muut lokitiedostot kuten palvelin- tai palomuurilokit.
- Kyselyt, palautekanavat.
- Monitorointi- ja valvontaratkaisut.
- Automaattiset hälytykset.
- Erilaiset dashboardit tai raportit.
- Automaattisesti tai manuaalisesti tehtävät toimenpiteet ja toimenpideohjeet.
- Kehitysideat / kehitystarpeet, mukaan lukien tarve poistaa jokin ohjelmointirajapinta käytöstä.

HYÖDYT

- Seuraamalla ohjelmointirajapinnoille asetettuja mittareita ja muita seurantakohteita organisaatio kykenee varmistamaan toimivatko ohjelmointirajapinnat odotetulla tavalla ja täyttyvätkö ohjelmointirajapinnoille asetetut ei-toiminnalliset vaatimukset, kuten palvelutaso, tietoturva tai käytettävyys.
- Lisäksi seurannan avulla organisaatio kykenee myös varmistamaan, saavutettiinko strategisella tasolla asetettuja tavoitteita vai ei.
- Seuranta edistää ohjelmointirajapintojen asiakaslähtöisyyttä ja yhteistyötä, uudelleenkäytettävyyttä, tietoturvaa ja tietosuojaa sekä laatua.

3.4 Yhteenveto periaatteista

Kuva 12. Yhteenveto periaatteista



LÄHTEET

Preston-Werner, Tom. 2021. Semantic Versioning 2.0.0. [Online] 2021. [Viitattu: 21. 6 2021.] https://semver.org/.

6Aika-kaupungit. 2016. Palauterajapinta, 6Aika. [Online] 2016. [Viitattu: 12. 11 2021.] https://github.com/6aika/api-palaute.

APIOps Cycles TM. 2021. APIOps Cycles for Lean API Development. [Online] 2021. [Viitattu: 16. 6 2021.] https://www.apiopscycles.com/.

CSC – Tieteen tietotekniikan keskus Oy. 2021. Säilytys- ja siirtokelpoiset tiedostomuodot. [Online] 2021. [Viitattu: 27. 10 2021.] https://www.digitalpreservation.fi/specifications/fileformats.

Department of Defence, United States of America. 2021. DoD Enterprise DevSecOps Fundamentals. [Online] 2021. [Viitattu: 21. 6 2021.] https://software.af.mil/wp-content/uploads/2021/05/DoD-Enterprise-DevSecOps-2.0-Fundamentals.pdf.

DevOps.com. 2021. DevOps.com Where the World Meets DevOps. [Online] 2021. [Viitattu: 23. 8 2021.] https://devops.com/.

DevSecOps. 2021. Manifesto. [Online] 2021. [Viitattu: 5. 8 2021.] https://www.devsecops.org/.

Digi- ja väestötietovirasto. 2021a. Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI. [Online] 2021a. [Viitattu: 21. 6 2021.] https://dvv.fi/vahti.

—. 2021b. Suomi.fi-palveluväylä. [Online] 2021b. [Viitattu: 23. 8 2021.] https://www.suomi.fi/palvelut/suomi-fi-palveluvayla-digi-ja-vaestotietovirasto/4ab88971-b9fb-443c-99aa-bc361bac7548.

—. 2021c. Tunnistus. [Online] 2021c. [Viitattu: 5. 8 2021.] https://dvv.fi/tunnistus.

—. 2021d. Valtuudet. [Online] 2021d. [Viitattu: 5. 8 2021.] https://dvv.fi/valtuudet.

—. 2021e. Yhteentoimivuusalusta. [Online] 2021e. [Viitattu: 21. 6 2021.] https://dvv.fi/yhteentoimivuusalusta.

—. 2022a. Palvelutietovaranto. [Online] 2022a. [Viitattu 14.2.2022.] https://dvv.fi/palvelutietovaranto.

—. 2022b. Avoindata.fi -palvelu. [Online] 2022b. [Viitattu 14.2.2022.] https://www.avoindata.fi/fi.

Digime-tietoarkkitehtuuriryhmä. 2021. Digime-standardisalkku. [Online] 2021. [Viitattu: 27. 10 2021.] https://www.doria.fi/handle/10024/180685.

Digitaalinen Helsinki. 2021. Helsingin datastrategia. [Online] 2021. [Viitattu: 17. 6 2021.] https://digi.hel.fi/esittely/helsinki-datastrategia/.

eOppiva. 2021a. Johdanto kokonaisarkkitehtuuriin. [Online] 2021a. [Viitattu: 21. 6 2021.] https://www.eoppiva.fi/kurssit/johdanto-kokonaisarkkitehtuuriin/#/.

—. 2021b. Kokonaisarkkitehtuurin mallintaminen. [Online] 2021b. [Viitattu: 21. 6 2021.] https://www.eoppiva.fi/kurssit/kokonaisarkkitehtuurin-mallintaminen/#/.

Euroopan Komissio. 2017. Eurooppalaiset yhteentoimivuusperiaatteet – täytäntöönpanostrategia. [Online] 2017. [Viitattu: 15. 9 2021.] https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:52017DC0134&from=EN.

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. 2016/679. EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). [Online] 2016/679. [Viitattu: 9. 6 2021.] https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32016R0679.

Euroopan parlamentin ja neuvoston direktiivi 2007/2/EY. 2019. EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI 2007/2/EY Euroopan yhteisön paikkatietoinfrastruktuurin (INSPIRE) perustamisesta. [Online] 2019. [Viitattu: 23. 8 2021.] https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A32007L0002.

Fintraffic. 2021. Liikenteen avoin data ja rajapinnat. [Online] 2021. [Viitattu: 19. 10 2021.] https://www.digitraffic.fi/.

Gartner. 2021. Full Life Cycle API Management Reviews and Ratings. [Online] 2021. [Viitattu: 21. 6 2021.] https://www.gartner.com/reviews/market/full-life-cycle-api-management.

GitHub. 2021. GitHub. [Online] 2021. [Viitattu: 30. 6 2021.] https://github.com/.

GraphQL Foundation. 2021. A query language for your API. [Online] 2021. [Viitattu: 21. 6 2021.] https://graphql.org/.

Hansel. 2021. Yhteishankinnat. [Online] 2021. [Viitattu: 4. 11 2021.] https://www.hansel.fi/yhteishankinnat/.

Helsingin kaupunginkanslia. 2020. Helsingin kaupungin palauterajapinta. [Online] 2020. [Viitattu: 12. 11 2021.] https://www.avoindata.fi/data/fi/dataset/helsingin-kaupungin-palauterajapinta.

HL7 Finland. 2021. Rajapintakartta. [Online] 2021. [Viitattu: 5. 8 2021.] http://www.hl7.fi/hl7-rajapintakartta/.

Honkanen, Mika. 2021. API-Suomi. [Online] 2021. [Viitattu: 30. 6 2021.] https://fi-fi.facebook.com/groups/apisuomi/.

Hornbeek, Marc. 2021. DevOps Testing. [Online] 2021. [Viitattu: 30. 6 2021.] https://devopsinstitute.com/wp-content/uploads/2018/03/DevOps-testing-ebook-online.pdf.

Hyvän Mitta. 2021. Mittareiden valinta. [Online] 2021. [Viitattu: 4. 11 2021.] https://www.hyvanmitta.fi/mita-mitataan/.
IBM. 2020. ETL (Extract, Transform, Load). [Online] 2020. [Viitattu: 5. 11 2021.] https://www.ibm.com/cloud/learn/etl.
ite wiki. 2021. DevOps. [Online] 2021. [Viitattu: 16. 6 2021.] https://www.itewiki.fi/opas/devops/.
Joint Research Centre (European Commission). 2020. An Application Programming Interfaces (APIs) framework for digital government. [Online] 2020. [Viitattu: 15. 9 2021.] https://op.europa.eu/en/publication-detail/-/publication/0e262d9b-ca32-11ea-adf7-01aa75ed71a1/language-en.
JSON Schema. 2021. JSON Schema. [Online] 2021. [Viitattu: 21. 6 2021.] https://json-schema.org/.
Julkisten hankintojen neuvontayksikkö. 2021. Julkisten hankintojen neuvontayksikkö. [Online] 2021. [Viitattu: 23. 8 2021.] https://www.hankinnat.fi/.
Kansallinen turvallisuusviranomainen, Ulkoministeriö. 2020. Katakri 2020 - tietoturvallisuuden auditointityökalu viranomaisille. [Online] 2020. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246.
Kansalliskirjasto. 2021. Finto.fi - keskitetty palvelu eri alojen yhteentoimiville sanastoille, ontologioille ja luokituksille. [Online] 2021. [Viitattu: 1. 11 2021.] https://finto.fi/fi/.
Kansalliskirjasto, Finna. 2021. Finnan avoin rajapinta. [Online] 2021. [Viitattu: 12. 11 2021.] https://www.kiwi.fi/display/Finna/Finnan+avoin+rajapinta.
Kuntaliitto. 2021. Yhteentoimivuustyö kunnissa. [Online] 2021. [Viitattu: 21. 6 2021.] https://www.youtube.com/watch?v=FNNL8K0EBCI.
Kyberturvallisuuskeskus. 2021a. Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat. [Online] 2021a. [Viitattu: 1. 7 2021.] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf.
—. 2021b. Luottamuksellinen viestintä. [Online] 2021b. [Viitattu: 25. 8 2021.] https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/luottamuksellinen-viestinta.
—. 2021. Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista. [Online] 2021. [Viitattu: 3.2.2022.] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Yhdyskaytavaratkaisuohje.pdf.
—. 2021c. Sähköinen tunnistaminen. [Online] 2021c. [Viitattu: 1. 7 2021.] https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen.
—. 2020. Turvallinen tuotekehitys - kohti hyväksyntää. [Online] 2020. [Viitattu: 25. 8 2021.] https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/turvallinen-tuotekehitys-kohti-hyvaksyntaa.
Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista. 571/2016. Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista. [Online] 571/2016. [Viitattu: 21. 6 2021.] https://finlex.fi/fi/laki/alkup/2016/20160571.
Laki julkisista hankinnoista ja käyttöoikeussopimuksista 1397/2016. 2016. Laki julkisista hankinnoista ja käyttöoikeussopimuksista. [Online] 2016. [Viitattu: 23. 8 2021.] https://www.finlex.fi/fi/laki/alkup/2016/20161397.
Laki paikkatietoinfrastruktuurista 421/2009. 2009. Laki paikkatietoinfrastruktuurista. [Online] 2009. [Viitattu: 23. 8 2021.] https://www.finlex.fi/fi/laki/alkup/2009/20090421.
Laki sähköisen viestinnän palveluista 7.11.2014/917. 2014. Laki sähköisen viestinnän palveluista. [Online] 2014. [Viitattu: 25. 8 2021.] https://www.finlex.fi/fi/laki/ajantasa/2014/20140917.
Maanmittauslaitos. 2021a. Paikkatietoalan standardit ja suositukset. [Online] 2021a. [Viitattu: 21. 6 2021.] https://www.maanmittauslaitos.fi/kartat-ja-paikkatieto/paikkatietojen-yhteentoimivuus/standardit-ja-suositukset.
—. 2021b. Rakennustietojen kyselypalvelu (WFS). [Online] 2021b. [Viitattu: 8. 6 2021.] https://www.maanmittauslaitos.fi/rakennustietojen-kyselypalvelu.
—. 2021c. Yhteistyöryhmät. [Online] 2021c. [Viitattu: 30. 6 2021.] https://www.maanmittauslaitos.fi/tietoa-maanmittauslaitoksesta/organisaatio/yhteistyoryhmat.
NIST, National Institute of Standards and Technology, U.S. Department of Commerce. 2020. Zero Trust Architecture. [Online] 8 2020. [Viitattu: 27. 10 2021.] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.
OECD. 2002. Glossary of statistical terms: Quality - ISO. [Online] 2002. [Viitattu: 9. 6 2021.] https://stats.oecd.org/glossary/detail.asp?ID=5150.
Open API Initiative. 2021. Open API. [Online] 2021. [Viitattu: 21. 6 2021.] https://www.openapis.org.
OWASP Cheat Sheet Series. 2021a. REST Security Cheat Sheet. [Online] 2021a. [Viitattu: 5. 8 2021.] https://cheatsheetseries.owasp.org/cheatsheets/REST_Security_Cheat_Sheet.html#https.
—. 2021b. Transport Layer Protection Cheat Sheet. [Online] 2021b. [Viitattu: 5. 8 2021.] https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html.
OWASP. 2019. OWASP API Security Top 10 2019 The ten most critical API security risks. [Online] 2019. [Viitattu: 21. 6 2021.] https://github.com/OWASP/API-Security/raw/master/2019/en/dist/owasp-api-security-top-10.pdf.
RAML. 2021. The simplest way to model APIs. [Online] 2021. [Viitattu: 1. 7 2021.] https://raml.org/.

Rautio, Pasi. 2015. Strategisten tavoitteiden toteutumisen mittaaminen. [Online] 2015. [Viitattu: 4. 11 2021.] https://www.theseus.fi/handle/10024/89635.
Sharma, Nitin ja Tutorials Point. 2019. What is the difference between ODBC and JDBC. [Online] 2019. [Viitattu: 4. 11 2021.] https://www.tutorialspoint.com/what-is-the-difference-between-odbc-and-jdbc.
Software Testing Fundamentals. 2021. Sotware Testing Fundamentals. [Online] 2021. [Viitattu: 30. 6 2021.] https://softwaretestingfundamentals.com/.
Software Testing Materials. 2020. A Comprehensive API Testing Guide. [Online] 2020. [Viitattu: 30. 6 2021.] https://www.softwaretestingmaterial.com/api-testing/.
Suomen standardisoimisliitto SFS Ry. 2021a. Standardisointiryhmät. [Online] 2021a. [Viitattu: 23. 8 2021.] https://sfs.fi/osallistu-ja-vaikuta/standardisointiryhmat/?fwp_aihealueet=tieto-ja-viestintatekniikka.
—. 2021b. Tieto- ja viestintätekniikka. [Online] 2021b. [Viitattu: 23. 8 2021.] https://sfs.fi/osallistu-ja-vaikuta/aihealueet/tieto-ja-viestintatekniikka/.
Swagger. 2021. Swagger UI. [Online] 2021. [Viitattu: 21. 6 2021.] https://swagger.io/tools/swagger-ui/.
TechTarget. 2017. synchronous/asynchronous API. [Online] 2017. [Viitattu: 4. 11 2021.] https://whatis.techtarget.com/definition/synchronous-asynchronous-API.
Tiedonhallintalaki 906/2019. 2019. Laki julkisen hallinnon tiedonhallinnasta. [Online] 2019. [Viitattu: 8. 6 2021.] https://www.finlex.fi/fi/laki/alkup/2019/20190906.
TIEKE Tietoyhteiskunna Kehittämiskeskus Ry. 2021. Verkkolaskufoorumi. [Online] 2021. [Viitattu: 30. 6 2021.] https://tieke.fi/palvelut/liiketoimintapalvelut/verkkolaskufoorumi/.
Tietosuojalaki. 5.12.2018/1050. Tietosuojalaki. [Online] 5.12.2018/1050. [Viitattu: 9. 6 2021.] https://www.finlex.fi/fi/laki/ajantasa/2018/20181050.
Tietosuojavaltuutetun toimisto. 2021. Pseudonymisoidut ja anonymisoidut tiedot. [Online] 2021. [Viitattu: 25. 8 2021.] https://tietosuoja.fi/pseudonymisointi-anonymisointi.
Tilastokeskus. 2021. Tietoaineistojen laatukriteerit. [Online] 2021. [Viitattu: 21. 6 2021.] https://www.stat.fi/org/vuosiohjelma/tietoaineistojen-laatukriteerit.html.
Traficom. 2021. Traficom Avoin Data API. [Online] 2021. [Viitattu: 21. 6 2021.] https://opendata.traficom.fi/swagger/ui/index.
Traficom, Kyberturvallisuuskeskus. 2021. s.l. : Kyberturvallisuuskekus, 2021. (Online) 2021. (Viitattu 20.1.2022). Tunnisteet ja tietosuoja, anonymisointi ja sen rajat. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Tunnisteet%20ja%20tietosuoja.pdf.
Vaccari, L;ym. 2020. Application Programming Interfaces in Governments: Why, what and how. [Online] 2020. [Viitattu: 30. 6 2021.] https://publications.jrc.ec.europa.eu/repository/handle/JRC120429. ISBN 978-92-76-18981-7.
Valtioneuvosto. 2019:31. Pääministeri Sanna Marinin hallituksen ohjelma 10.12.2019. Osallistava ja osaava Suomi - sosiaalisesti, taloudellisesti ja ekologisesti kestävä yhteiskunta. [Online] 2019:31. [Viitattu: 8. 6 2021.] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161931/VN_2019_31.pdf?sequence=1&isAllowed=y.
Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa. 1101/2019. Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa. [Online] 1101/2019. [Viitattu: 30. 6 2021.] https://finlex.fi/fi/laki/alkup/2019/20191101.
Valtiovarainministeriö. 2021a. Tiedon hyödyntämisen ja avaamisen hanke. [Online] 2021a. [Viitattu: 8. 6 2021.] https://vm.fi/tiedon-hyodyntaminen-ja-avaaminen1.
—. 2021b. Tiedon yhteentoimivuus. [Online] 2021b. [Viitattu: 9. 6 2021.] https://vm.fi/tiedon-yhteentoimivuus.
—. 2022. Julkisen hallinnon tiedonhallintakartta tutkihallintoa.fi -palvelussa. [Online] 2022. [Viitattu 14.2.2022.] https://www.tutkihallintoa.fi/tiedonhallintakartta/.
Valtiovarainministeriö, Tiedonhallintalautakunta. 2021:21. Suositus teknisistä rajapinnoista ja katseluyhteyksistä. [Online] 2021:21. [Viitattu: 9. 6 2021.] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163070/VM_2021_21.pdf?sequence=1&isAllowed=y. ISBN pdf: 978-952-367-489-9.
—. 2020:29. Suositus tiedonhallintamallista. [Online] 2020:29. [Viitattu: 9. 6 2021.] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162176/VM_2020_29.pdf?sequence=1&isAllowed=y. ISBN PDF: 978-952-367-328-1.
—. 2020:19. Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. [Online] 2020:19. [Viitattu: 9. 6 2021.] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162154/VM_2020_19.pdf?sequence=1&isAllowed=y. ISBN PDF: 978-952-367-292-5.
—. 2020-2021. Tiedonhallintalautakunnan suositukset. [Online] 2020-2021. [Viitattu: 8. 6 2021.] https://vm.fi/suositukset.
—. 2021:65. Valtiovarainministeriön julkaisuja – 2021:65 Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta. [Online] 2021:65. [Viitattu: 8. 6 2021.] https://julkaisut.valtioneuvosto.fi/handle/10024/163596. ISBN:978-952-367-897-2.
Valtiovarainministeriö, VAHTI. 22/2017. VAHTI 22/2017 Ohje riskienhallintaan. [Online] 22/2017. https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-222017-ohje-riskienhallintaan.

—. 22/2017. VAHTI 22/2017 Ohje riskienhallintaan - liitteet 1 - 6. [Online] 22/2017. https://www.suomidigi.fi/sites/default/files/2020-06/Liitteet_VM22_2017.pdf.
Valtori. 2021. Integraatiopalvelut. [Online] 2021. [Viitattu: 21. 6 2021.] https://valtori.fi/yhteinen-integraatioalusta-via-julkiset-varmenteet.
Varsinais-Suomen liitto. 2021. Avoimen tiedon verkosto. [Online] 2021. [Viitattu: 30. 6 2021.] https://kumppanuusfoorumi.fi/foorumi/avoimen-tiedon-verkosto/.
Verohallinto. 2019. API-kehittäminen Verolla. [Online] 2019. [Viitattu: 17. 6 2021.] http://131.207.14.19/contentassets/5389e8bf012445db8fb5865ad0fe745e/10.-api-kehitt%C3%A4minen_verolla.pdf.
—. 2021a. Tulorekisterin tekninen rajapinta. [Online] 2021a. [Viitattu: 9. 6 2021.] https://www.vero.fi/tulorekisteri/yritykset-ja-organisaatiot/suorituksen-maksajat/ilmoittamisen-kanavat/tekninen-rajapinta/.
—. 2021b. Vero API. [Online] 2021b. https://www.vero.fi/tietoa-verohallinnosta/kehittaja/veron-rajapintapalvelut/vero-api/.
—. 2021c. Veronumeron rekisteröinnin tarkistus. [Online] 2021c. [Viitattu: 8. 6 2021.] https://avoinomavero.vero.fi/_/.
—. 2021d. Veronumerorekisteri. [Online] 2021d. https://www.suomi.fi/palvelut/veronumerorekisteri-verohallinto/57063087-94c6-4c6e-9e2e-545bb5128010.
Väylävirasto. 2021. Väyläviraston avoimet rajapinnat. [Online] 2021. [Viitattu: 8. 6 2021.] https://vayla.fi/vaylista/aineistot/avoindata/rajapinnat.
W3Schools. 2021a. JSON - Introduction. [Online] 2021a. [Viitattu: 21. 6 2021.] https://www.w3schools.com/js/js_json_intro.asp.
—. 2021b. RESTful Web services. [Online] 2021b. [Viitattu: 21. 6 2021.] REST https://www.w3schools.in/restful-web-services/intro/.
—. 2021c. Software Testing Tutorial Library. [Online] 2021c. [Viitattu: 30. 6 2021.] https://www.w3schools.in/software-testing/.
—. 2021d. XML Schema Tutorial. [Online] 2021d. [Viitattu: 21. 6 2021.] https://www.w3schools.com/xml/schema_intro.asp.
—. 2021e. XML Soap. [Online] 2021e. [Viitattu: 30. 6 2021.] https://www.w3schools.com/xml/xml_soap.asp.
—. 2021f. XML Tutorial. [Online] 2021f. [Viitattu: 21. 6 2021.] https://www.w3schools.com/xml/.

Liitteet

Liite 1: Esimerkki ohjelmointirajapintojen riskiarvioinnista tietoriskianalyysin avulla

Tiedonhallintalain[124] mukaan myös ohjelmointirajapintoihin ja niiden käsittelemiin tietoihin kohdistuvat olennaiset riskit on selvitettävä ja tunnistettuihin riskeihin on mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Julkisen hallinnon riskienhallinnan tehostamista ja yhdenmukaistamista varten Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI) on laatinut riskienhallintaohjeen[125], jota voi hyödyntää myös ohjelmointirajapintoihin liittyvässä riskienhallinnassa[126]. Itse ohje kuvaa yleisen riskienhallintaprosessin ja ohjeen liitteessä 4[127] kuvataan riskienhallinnan standardeja ja hyviä käytäntöjä.

Euroopan komissio on omassa julkisen hallinnon ohjelmointirajapintojen käyttöönottoon liittyvässä tutkimuksessaan tunnistanut joukon ohjelmointirajapintoihin liittyviä riskejä ja niiden hallintakeinoja[128]. Tutkimuksen mukaan ohjelmointirajapinnat aiheuttavat teknisiä, organisatorisia, juridisia ja taloudellisia riskejä, jotka on tunnistettava ja hallittava osana organisaation muuta riskienhallintaa.

Tässä yhteydessä käytetään esimerkkinä VAHTI-ohjeen liitteessä 4 kuvattua tietoriskianalyysiä, jota voidaan käyttää ohjelmointirajapinnan tai ohjelmointirajapintojen muodostaman palvelukokonaisuuden arvioimiseen tietoturvallisuuden peruskäsitteiden kautta ja sitä kautta kartoittamaan todennäköisimmät riskit ja uhat sekä kuvaamaan niiden pahimmat seuraukset.

124 Tiedonhallintalaki, 4 luku, 13 §, (Tiedonhallintalaki 906/2019, 2019)

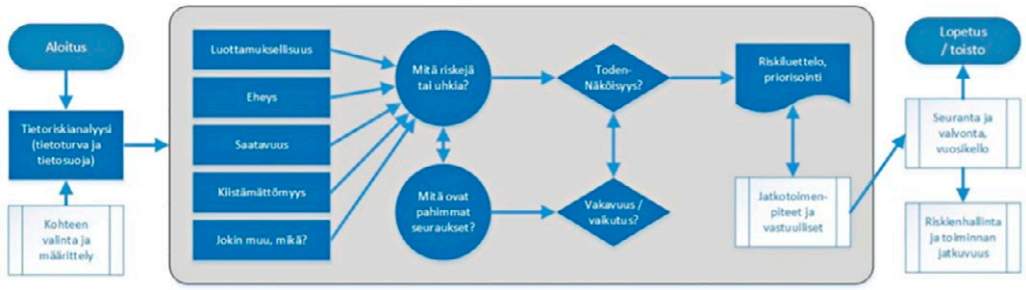
125 VAHTI 22/2017 Ohje riskienhallintaan, (Valtiovarainministeriö, VAHTI, 22/2017)

126 Tiedonhallintalautakunnan suositus teknisistä rajapinnoista ja katseluyhteyksistä, s 16, (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:21)
Katakri 2020 – tietoturvallisuuden auditointityökalu viranomaisille, T-03, s. 11, (Kansallinen turvallisuusviranomainen, Ulkoministeriö, 2020)

127 VAHTI 22/2017 Ohje riskienhallintaan – liite 4, (Valtiovarainministeriö, VAHTI, 22/2017)

128 European Commision Joint Research Centre, Application Programming Interfaces in Governments: Why, what and how, s. 53–55 (Vaccari, et al., 2020)

Kuva 13. Tietoriskianalyysi VAHTI 22/2017 -ohjeen liitteen 4 mukaan



Tietoriskianalyysi alkaa valitsemalla riskienhallinnan kohteeksi ohjelmointirajapinta tai ohjelmointirajapintojen muodostama palvelukokonaisuus ja tunnistamalla siinä käsiteltävät tiedot, tietojen luokittelu sekä tiedon omistajat.

Tietoriskianalyysin voi toteuttaa arvioimalla riskejä ja uhkia, jotka kohdistuvat ohjelmointirajapinnan käsittelemän tiedon luottamuksellisuuteen, eheyteen, saatavuuteen ja kiistämättömyyteen. Muita riskiarvioinnin näkökulmia ovat esimerkiksi ohjelmointirajapinnan kriittisyys organisaation toimintaan, jatkuvuuteen ja toipumiseen liittyvät varautumisen vaatimukset sekä sisäiset ja ulkoiset riippuvuudet.

Näkökulmien valinnan jälkeen arvioidaan, mitä riskejä tai uhkia ohjelmointirajapintoihin liittyen tunnistetaan sekä mitkä ovat pahimmat seuraukset, mikäli riski tai uhka toteutuu. Näin tunnistetuille riskeille arvioidaan todennäköisyys ja vakavuus, joiden perusteella saadaan priorisoitu riskiluettelo (yleensä priorisointi = todennäköisyys x vakavuus).

Lopuksi jokaiselle priorisoidulle riskille määritetään riskinhallintatoimenpiteet, toimenpiteistä vastuulliset henkilöt sekä riskin seurantamenettelyt ja -päivämäärät. Riskienhallintatoimenpiteet voivat olla sekä hallinnollisia (esimerkiksi ohjelmointirajapinnan kehitysprosessiin liittyviä toimenpiteitä, kuten testaus- ja katselmointikäytäntöjen määrittelyjä) että teknisiä (esimerkiksi ohjelmointirajapinnan testausautomaation ja teknisten tietoturvakontrollien toteuttamista).

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

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

ISSN 1797-9714 (pdf)
ISBN 978-952-367-907-8 (pdf)

Helmikuu 2022