VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

API-principer för den offentliga förvaltningen

Finansministeriet Helsingfors 2021

Innehåll

1 Inledning

Statsminister Sanna Marins regeringsprogram[1] har som mål att fördjupa ledningen av informationspolitiken och att göra öppenhet i den offentliga informationen till en bärande princip i hela informationspolitiken. Utgångspunkten är bland annat att offentliga aktörer öppnar offentliga gränssnitt, om det inte finns särskild anledning att hålla dem stängda, och öppna gränssnitt förutsätts i offentliga systemupphandlingar. Finansministeriets projekt Utnyttja och öppna information genomför mål i statsminister Marins regeringsprogram som gäller informationspolitik och utnyttjandet och öppnandet av information[2]. Projektet har tillsatts för perioden 30.4.2020–31.12.2022. Syftet med projektet är bland annat att främja utnyttjandet av information och funktioner på ett enhetligt sätt genom applikationsprogrammeringsgränssnitt (API).

I detta dokument presenteras principerna och stödmaterialet för utvecklingen av applikationsprogrammeringsgränssnitt (API) inom den offentliga förvaltningen. Principerna utgör de gemensamma anvisningarna och rekommendationerna för API-utvecklingen och främjandet av digitaliseringen inom den offentliga förvaltningen. Stödmaterialet och exemplen erbjuder mer praktiknära instruktioner i syfte att stödja ibruktagandet.

Principerna stödjer genomförandet av de krav på informationsöverföringsmetoden som föreskrivs i lagen om informationshantering[3]. Som referensram för principerna har använts Europeiska kommissionens API Framework[4], och bland annat den europeiska interoperabilitetsramen om teknisk och semantisk interoperabilitet beaktats[5]. Vid beredningen av principerna och stödmaterialet har dessutom beaktats sektorsspecifik reglering, såsom direktivet INSPIRE[6], informationshanteringsnämndens rekommendationer[7] och de strategiska nationella målen för utnyttjande och öppnande av information[8].

Principerna och stödmaterialet tar ställning till gränssnittsutvecklingen på ett bredare plan än till exempel informationshanteringsnämndens nuvarande rekommendationer.

Myndigheterna kan fortsätta att utveckla principerna för sina egna behov, till exempel när det gäller deras förpliktande karaktär.

---

[1] Statsminister Sanna Marins regeringsprogram (Valtioneuvosto, 2019:31)
[2] Projektet Utnyttja och öppna information (Valtiovarainministeriö, 2021a)
[3] Lagen om informationshantering, 22 § och 24 § (Tiedonhallintalaki 906/2019, 2019)
[4] An Application Programming Interface (API) framework for digital government. (Joint Research Centre (European Commission), 2020)
[5] Europeiska interoperabilitetsramen - genomförandestrategi. (Euroopan Komissio, 2017)
[6] INSPIRE-direktivet (Euroopan parlamentin ja neuvoston direktiivi 2007/2/EY, 2019) och det nationella genomförandet (Laki paikkatietoinfrastruktuurista 421/2009, 2009)
[7] Informationshanteringsnämndens rekommendationer (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020-2021)
[8] De nationella strategiska målen för utnyttjande och öppnande av information (Valtiovarainministeriö, 2021b) (Källhänvisningen är bristfällig och läggs till när de strategiska målen har publicerats.)

1.1 Mål

Syftet med principerna är att främja utbudet och användningen av den offentliga förvaltningens information och funktioner primärt med hjälp av applikationsprogrammeringsgränssnitt. Syftet med principerna är att öka kundfokusen, samarbetet, den semantiska och tekniska interoperabiliteten, återanvändbarheten, dataskyddet och informationssäkerheten samt kvaliteten vid utvecklingen av API:er.

Kundfokus betyder att hänsyn tas till behoven hos applikationsprogrammeringsgränssnittets potentiella användare under hela gränssnittets livscykel från kartläggningen av behoven till urbruktagningen. Gränssnitt som utvecklas med kundfokus tillgodoser användarnas behov och utvecklas kontinuerligt i en riktning som betjänar användarna allt bättre. Kundfokusen ökar användarnas belåtenhet och höjer programmeringssnittens driftsgrad.

Kundfokus kräver **samarbete** mellan dem som tillhandahåller information och gränssnitt och dem som använder gränssnitten. Samarbetet kan vara internt i organisationen eller externt med andra organisationer. Det interna samarbetet täcker samarbetet mellan olika nivåer, team och enheter i organisationen. Det externa samarbetet kan vara samarbete mellan aktörer på den offentliga sektorn eller mellan aktörer i den offentliga och privata sektorn, eller samarbete med medborgare. Samarbetet främjar den kundorienterade utvecklingen och gör det möjligt att dela kunnande, erfarenheter och lösningar mellan olika aktörer.

Återanvändbarhet innebär att applikationsprogrammeringsgränssnitten och de uppgifter och funktioner som de erbjuder kan hittas och användas vid genomförandet av nya lösningar. Det överlappande arbetet och de överlappande lösningarna minskar, utvecklingsarbetet blir snabbare och produktiviteten ökar när det blir möjligt att utveckla nya lösningar på existerande information, funktioner och applikationsprogrammeringsgränssnitt.

Teknisk interoperabilitet betyder att olika tekniker för dataöverföring sammanpassas[9]. **Semantisk interoperabilitet** innebär att informationens betydelse bevaras och förstås genom hela utbytet mellan parterna, med andra ord att ”det som skickas är det som förstås[10]. Med hjälp av tekniskt och semantiskt interoperabla applikationsprogrammeringsgränssnitt blir det lättare att överföra information, samtidigt som utvecklingsarbetet blir snabbare och produktiviteten ökar.

[9] Definition av teknisk interoperabilitet (Valtiovarainministeriö, 2021c)
[10] Definition av semantisk interoperabilitet (Valtiovarainministeriö, 2021c)

Med **informationssäkerhet** avses att hänsyn tas till de behandlade uppgifternas integritet, konfidentialitet och tillgänglighet under hela applikationsprogrammeringsgränssnittets livscykel. Med **dataskydd** avses att de personuppgifter som behandlas i applikationsprogrammeringsgränssnitten har skyddats i enlighet med föreskrifterna.

Med **kvalitet** avses att applikationsprogrammeringsgränssnittens egenskaper eller kapaciteter tillgodoser användarnas behov och förväntningar[11]. Genom högklassiga applikationsprogrammeringsgränssnitt ökar användarnas belåtenhet och applikationsprogrammeringsgränssnittens driftsgrad ökar. Kvaliteten gör dessutom utvecklingsarbetet snabbare och ökar därigenom produktiviteten.

1.2 Målgrupp

I principernas målgrupp ingår:

- organisationerna inom den offentliga förvaltningen, till exempel statliga ämbetsverk och inrättningar, kommuner och samkommuner samt högskolor och andra läroanstalter.

- företag, sammanslutningar och andra aktörer som behandlar den offentliga förvaltningens information eller utför ett offentligt förvaltningsuppdrag.

- företag, sammanslutningar och andra aktörer som lämnar tjänster eller lösningar för informationsbehandling eller informationshantering till organisationer inom den offentliga förvaltningen.

1.3 Avgränsningar

Principerna gäller inte gränssnitt som anknyter till användargränssnitt som avsetts för slutanvändare.

Principerna är inte en heltäckande handbok eller designguide för applikationsprogrammeringsgränssnitt. I principerna nämns inte tekniker, dataöverföringsformat eller datamodeller som ska användas, men ges approximativa exempel på dem.

Principerna innehåller inte heller anvisningar eller specifikationer för enskilda branscher, men sådana kan utvecklas branschvis ovanpå principerna.

[11] Definitionen av kvalitet bygger på OECD:s ISO-definition (OECD, 2002)

2 Vad är API:er?

2.1 Definitioner

Applikationsprogrammeringsgränssnitt, dvs. API:er (Application Programming Interface) är dokumenterade gränssnitt med vilka programvara, applikationer eller system kan utbyta information eller funktioner med varandra[12]. Med API, dvs. applikationsprogrammeringsgränssnitt, avses i detta dokument samma sak som med *tekniskt gränssnitt*, som definieras i lagen om informationshantering[13].

Definierat på detta sätt täcker begreppet applikationsprogrammeringsgränssnitt både de webbaserade API:erna REST, SOAP och GraphQL och gränssnitt som bygger på fil- och databasbaserade protokoll och på andra protokoll. Det väsentliga är att **applikationsprogrammeringsgränssnittet erbjuder information eller en funktion i ett maskinläsbart, dokumenterat format på så sätt att ett annat program, en annan applikation eller ett annat system kan använda det programmässigt.**

Det gäller att observera att begreppet applikationsprogrammeringsgränssnitt inte avser användargränssnitt som är avsedda för slutanvändare. Användaren av ett applikationsprogrammeringsgränssnitt är alltid ett annat program eller system eller en annan applikation eller applikationskomponent.

2.2 Värdekedja

Applikationsprogrammeringsgränssnitt kan ses som separata produkter som förknippas med en värdekedja[14] (bild 1).

Värdekedjan börjar med en *leverantör av en digital nyttighet*, som innehar en produkt, en digital nyttighet som ger en annan aktör mervärde. Den digitala nyttigheten kan utgöras av till exempel uppgifter, såsom statistik- eller registeruppgifter eller en funktion, såsom kalkylering av skatteprocent eller en ramverksmodifierare.

En *leverantör av ett applikationsprogrammeringsgränssnitt* tillhandahåller ett applikationsprogrammeringsgränssnitt via vilket andra aktörer kan utnyttja den produkt som leverantören av

[12] Definitionen följer definitionen i Europeiska unionens publikation, sid. 18–19 (Vaccari, et al., 2020)
[13] Lagen om informationshantering, 2 § punkt 11 (Tiedonhallintalaki 906/2019, 2019)
[14] Värdekedjan följer den värdekedja som presenteras i Europeiska unionens publikation, sid. 20 (Vaccari, et al., 2020)

den digitala nyttigheten innehar. Applikationsprogrammeringsgränssnittets leverantör kan vara samma aktör eller en annan aktör än leverantören av en digital nyttighet.

Applikationsprogrammeringsgränssnittets leverantör använder gränssnittet och den information eller funktion som den omfattar i sin egen applikation eller tjänst. Den som utnyttjar applikationsprogrammeringsgränssnittet kan vara samma aktör som den som tillhandahåller applikationsprogrammeringsgränssnittet eller en annan aktör.

En applikation eller tjänst kan ytterligare ha en *slutanvändare*. Slutanvändarna utnyttjar således inte de egentliga applikationsprogrammeringsgränssnitten direkt, utan alltid via någon annan applikation eller tjänst.

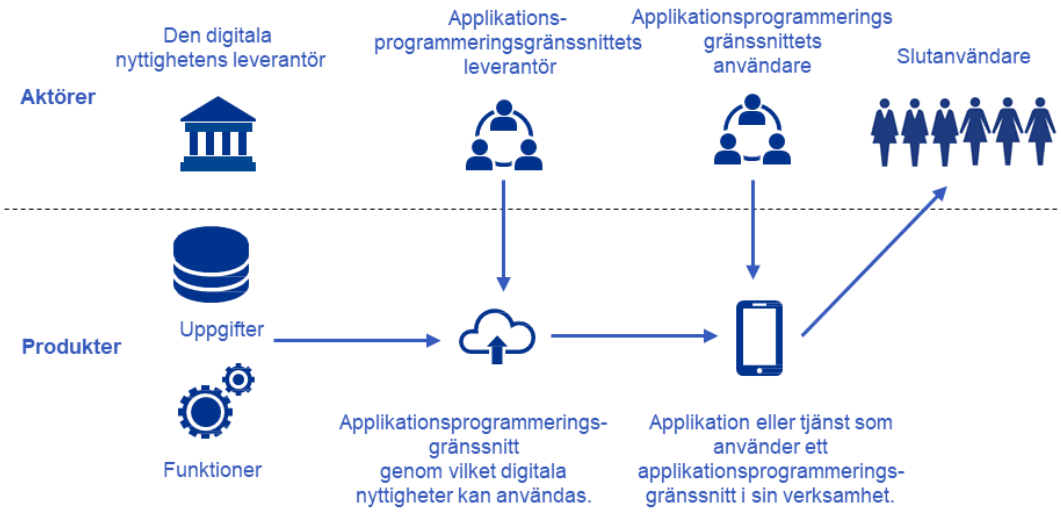

Bild 1 - Värdekedjan för en API[15]

EXEMPEL

- Skatteförvaltningen innehar information om personernas skattenummer och deras giltighet[16]. Skatteförvaltningen är leverantör av en digital nyttighet.
- Skatteförvaltningen har utvecklat ett applikationsprogrammeringsgränssnitt[17] via vilka andra aktörer med hjälp av ett program kan kontrollera om ett bestämt skattenummer

[15] Värdekedjan följer den värdekedja som presenteras i Europeiska kommissionens publikation, sid. 20 (Vaccari, et al., 2020).
[16] Skatteförvaltningens skattenummerregister (Verohallinto, 2021d)
[17] Skatteförvaltningens Vero API (Verohallinto, 2021b)

är i kraft eller inte. Skatteförvaltningen är leverantören av applikationsprogrammeringsgränssnittet.

- En aktör inom den privata sektorn utvecklar ett informationssystem med hjälp av vilken det är möjligt att administrera passerkort till byggarbetsplatser. När ett nytt passerkort utfärdas, kontrollerar informationssystemet med hjälp av det applikationsprogrammeringsgränssnitt som Skatteförvaltningen tillhandahåller att personens skattenummer är i kraft. I detta fall är aktören i den privata sektorn applikationsprogrammeringsgränssnittets användare.

- Byggföretagets anställda, till exempel byggarbetsplatschefer använder informationssystemet för att administrera passerkort. De är slutanvändare.

- Skatteförvaltningen erbjuder också ett webbgränssnitt med vilken det är möjligt att kontrollera skattenumret manuellt till exempel med en webbläsare eller mobilutrustning[18]. I det här fallet tillhandahåller Skatteförvaltningen en applikation eller tjänst direkt till slutanvändare. Om Skatteförvaltningen använder sitt eget applikationsprogrammeringsgränssnitt för kontroll av ett skattenummer via webbgränssnittet, är också Skatteförvaltningen en av användarna av dess eget applikationsprogrammeringsgränssnitt.

2.3 Typning

Applikationsprogrammeringsgränssnitten kan vara interna eller externa till sin typ. I tabell 1 presenteras de olika typerna av applikationsprogrammeringsgränssnitt och deras allmänna egenskaper.

Tabell 1 - API typer

Applikationsprogrammeringsgränssnittets typ		Begränsning av användningen	Potentiell användare	Klassificering av de behandlade uppgifterna
INTERN	Intern API	Ja	Aktörer i den egna organisationen	Säkerhetsklassificerad information Sekretessbelagd information inkl. personuppgifter Offentlig information

[18] Webbgränssnittet som Skatteförvaltningen tillhandahåller (Verohallinto, 2021c)

EXTERN	Partner-API	Ja	Aktörer i den egna organisationen Andra aktörer inom den offentliga förvaltningen Andra aktörer inom den privata sektorn Andra aktörer	Säkerhetsklassificerad information Sekretessbelagd information inkl. personuppgifter Offentlig information
	Offentlig API	Nej	Vem som helst.	Offentlig information

Interna applikationsprogrammeringsgränssnitt (*interna API*) är endast avsedda för organisationens egen användning. Externa användningsgränssnitt kan vara begränsade för vissa aktörer (*partner-API*) eller obegränsade API:er som är öppna för alla (*offentlig API*).

I interna applikationsprogrammeringsgränssnitt och externa för vissa partner avsedda applikationsprogrammeringsgränssnitt är det möjligt att behandla offentlig information, sekretessbelagd information, personuppgifter eller säkerhetsklassificerad information. I offentliga applikationsprogrammeringsgränssnitt behandlas endast offentlig information.

I interna applikationsprogrammeringsgränssnitt och i applikationsprogrammeringsgränssnitt som är begränsade till vissa partner identifieras (autentiseras) gränssnittets användare och kontrolleras (auktoriseras) användarens åtkomsträttigheter. I offentliga applikationsprogrammeringsgränssnitt behövs åtkomstkontroll (auktorisering) inte eftersom endast offentlig information tillhandahålls. I vissa fall kan användaren identifieras (autentiseras) även i offentliga applikationsprogrammeringsgränssnitt, till exempel om man i uppföljnings- eller kommunikationssyfte vill samla in information om dem som använder applikationsprogrammeringsgränssnittet.

EXEMPEL

- En aktör, till exempel en kommun, ett statligt ämbetsverk eller en läroanstalt, kan ha egna register, till exempel ett kundregister eller elevregister. Aktören utvecklar ett applikationsprogrammeringsgränssnitt för sökning av information i registret. Med hjälp av gränssnittet kan aktörens övriga informationssystem eller applikationer söka information från registret i fråga med hjälp av vissa sökkriterier. Om applikationsprogrammeringsgränssnittet endast är avsett för aktörens egen användning är det fråga om en intern API.

- Lantmäteriverket tillhandahåller en förfrågningstjänst[19] med hjälp av vilken det är möjligt att fråga efter byggnaders identifierande uppgifter, egenskapsuppgifter och ägaruppgifter. Användningen av tjänsten kräver tillstånd från Myndigheten för digitalisering och befolkningsdata och är därför begränsad till vissa aktörer. Det är fråga om ett partner-API.

- Trafikledsverket erbjuder gränssnitt som är öppna för alla[20] och som kan användas för att ladda ned och granska geodatamaterial som anknyter till väg-, ban-, och farledsnätverket. Det är fråga om en offentlig API vars användning inte kräver registrering eller identifiering.

2.4 Livscykel

Applikationsprogrammeringsgränssnitt har en livscykel som börjar med behovskartläggningen för gränssnittet och slutar när applikationsprogrammeringsgränssnittet tas ur bruk. Livscykeln täcker alla moment mellan dessa två punkter: specifikation och planering, konkurrensutsättning och upphandling, genomförande och utveckling, drifttagning, administration och urbruktagning[21]. Livscykeln för ett applikationsprogrammeringsgränssnitt är iterativt, dvs. momenten upprepas till applikationsprogrammeringsgränssnittet med alla dess versioner har tagits ur bruk.

Det gäller att observera att applikationsprogrammeringsgränssnittets livscykel kan avvika från livscykeln för den information eller funktion som det tillhandahåller. Det är möjligt att applikationsprogrammeringsgränssnittets livscykel börjar först senare än livscykeln för den information eller funktion som det tillhandahåller. Det är möjligt att det inte sker några förändringar i informationens livscykel, men applikationsprogrammeringsgränssnittets egenskaper eller funktionaliteter utvecklas, nya versioner av det införs och gamla versioner tas ur bruk. Det är också möjligt att applikationsprogrammeringsgränssnittets livscykel slutar före livscykeln för den information eller funktion som det tillhandahåller till exempel på grund av att användningsbehovet slutar eller tekniken föråldras.

[19] Lantmäteriverkets förfrågningstjänst (Maanmittauslaitos, 2021b)
[20] Trafikledsverkets öppna gränssnitt (Väylävirasto, 2021)
[21] Följer livscykeln för ett informationssystemet, sid. 26 (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:61)

3 Principer

Principerna har fördelats på tre nivåer: strategisk, taktisk och operativ.

Principerna på strategisk nivå är avsedda för 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 avsedda för aktörer som utvecklar organisationens informationshantering. Principerna på taktisk nivå styr hur utvecklandet och helheten av applikationsprogrammeringsgränssnitt ska hanteras.

Principerna på operativ nivå är avsedda för aktörer som utvecklar och administrerar applikationsprogrammeringsgränssnitt. Principerna på operativ nivå styr hur enskilda applikationsprogrammeringsgränssnitt ska utvecklas och administreras.

Principerna presenteras i avsnitt 3.1, 3.2 och 3.3. Principerna stödjer uppnåendet av de uppsatta målen (bild 3). Målen per princip presenteras med symbolerna nedan.

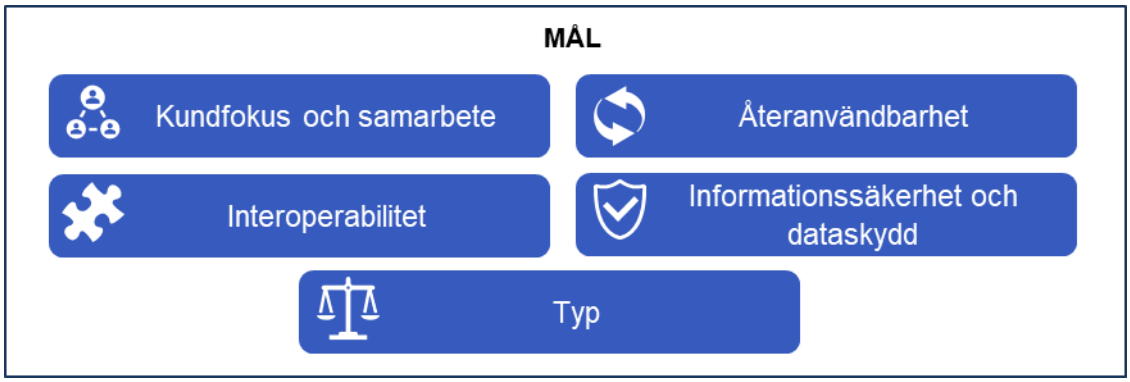

Bild 2 - Mål

3.1 Strategisk nivå

Bild 3 - Principer på strategisk nivå

Princip 1.1 Använd i regel applikationsprogrammerings-gränssnitt för att tillhandahålla och använda information

Identifiera informationsmaterial som är viktiga för verksamhetsprocesserna i din organisation och den nyttopotential som informationsmaterialen medför. Observera att informationsmaterialen kan vara organisationens egna eller tillhöra andra aktörer. Informationsmaterialens nyttopotential kan anknyta till utvecklingen av eller behoven inom organisationens eller intressentgruppers verksamhet. Information eller informationsmaterial som tillhandahålls eller utnyttjas via applikationsprogrammeringsgränssnitt kan definieras till exempel med följande frågor:

1. Vilken information finns det tillgång till i organisationen?

2. Vilken eller hurdan information behövs det mer av?

3. Vilken information stödjer kunskapsbaserad ledning?

4. Vilka informationsbehov har intressentgrupperna?

5. Vilken information behövs regelbundet, i maskinläsbart format eller så aktuellt som möjligt?

Definiera vilka eller hurdana informationsmaterial som tillhandahålls eller används internt och externt med hjälp av applikationsprogrammeringsgränssnitt. Internt kan tillhandahållandet och användningen utföras med interna applikationsprogrammeringsgränssnitt (intern API). Externt kan tillhandahållandet och användningen utföras med hjälp av partnergränssnitt (partner-API) eller offentliga gränssnitt (offentliga API) beroende på informationens klassificering.

Observera lagarna om rätten till åtkomst till information, överlåtelse av information och tillhandahållande av information i maskinläsbart format samt de skyldigheter som de ålägger[22]. Observera också eventuella behov att bearbeta informationsmaterialen, till exempel pseudonymisering eller anonymisering[23].

[22] Till exempel 22 § i informationshanteringslagen (Tiedonhallintalaki 906/2019, 2019) och Informationshanteringsnämndens rekommendation om tekniska gränssnitt och elektroniska förbindelser (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:21).
[23] Webbplatsen för pseudonymiserade och anonymiserade uppgifter (Tietosuojavaltuutetun toimisto, 2021)

RESULTAT

- Lista över informationsmaterial som eventuellt kan tillhandahållas eller användas via applikationsprogrammeringsgränssnitt.

STÖDMATERIAL

- *Rekommendation om informationshanteringsmodellen*[24].
- Koncept för verksamhetsmodell för att stödja identifieringen av information med nyttopotential och distributionen av dem[25].
- Informationshanteringskarta för identifiering av den nuvarande statusen för lagstadgade överlåtelser av information från förvaltningens lagstadgade informationslager[26].

Princip 1.2 Definiera målen för tillhandahållandet och användningen av applikationsprogrammeringsgränssnitt och skaffa tillräckliga resurser

Definiera målen för tillhandahållandet och användningen av applikationsprogrammeringsgränssnitt. Målen ska betjäna organisationens strategi och de ska vara i linje med målen för den övriga informationshanteringen. Målen ska vara realistiska i relation till organisationens storlek och kapaciteter. Definiera indikatorer som kan användas för att följa upp hur målen uppnås.

Skaffa de resurser som behövs för att uppnå målen. Resurserna kan vara till exempel personalresurser, rätt kompetens eller tekniska resurser. Anskaffningen och upprätthållandet av resurser och kompetens kräver finansiering. För en dialog med de team eller personer som ansvarar för informationshanteringen i organisationen om behoven av kompetens,

[24]Rekommendation om informationshanteringsmodellen (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:29)
[25] En länk läggs till senare efter att verksamhetsmodellen har publicerats
[26] En länk läggs till senare när kartan har publicerats (hösten 2021)

resurser och finansiering för att kunna identifiera och skaffa denna kompetens, dessa resurser och denna finansiering. Utveckla kompetensen hos personal i din egen organisation i den omfattning det är möjligt. Utnyttja existerande team eller personer som arbetar med informationshantering, applikationsutveckling eller integrationer.

I bild 4 presenteras ett exempel på mål, indikatorer och resurser för utvecklingen av applikationsprogrammeringsgränssnitt. I exempelbilden har målen härletts ur de strategiska målen för en fiktiv organisation.

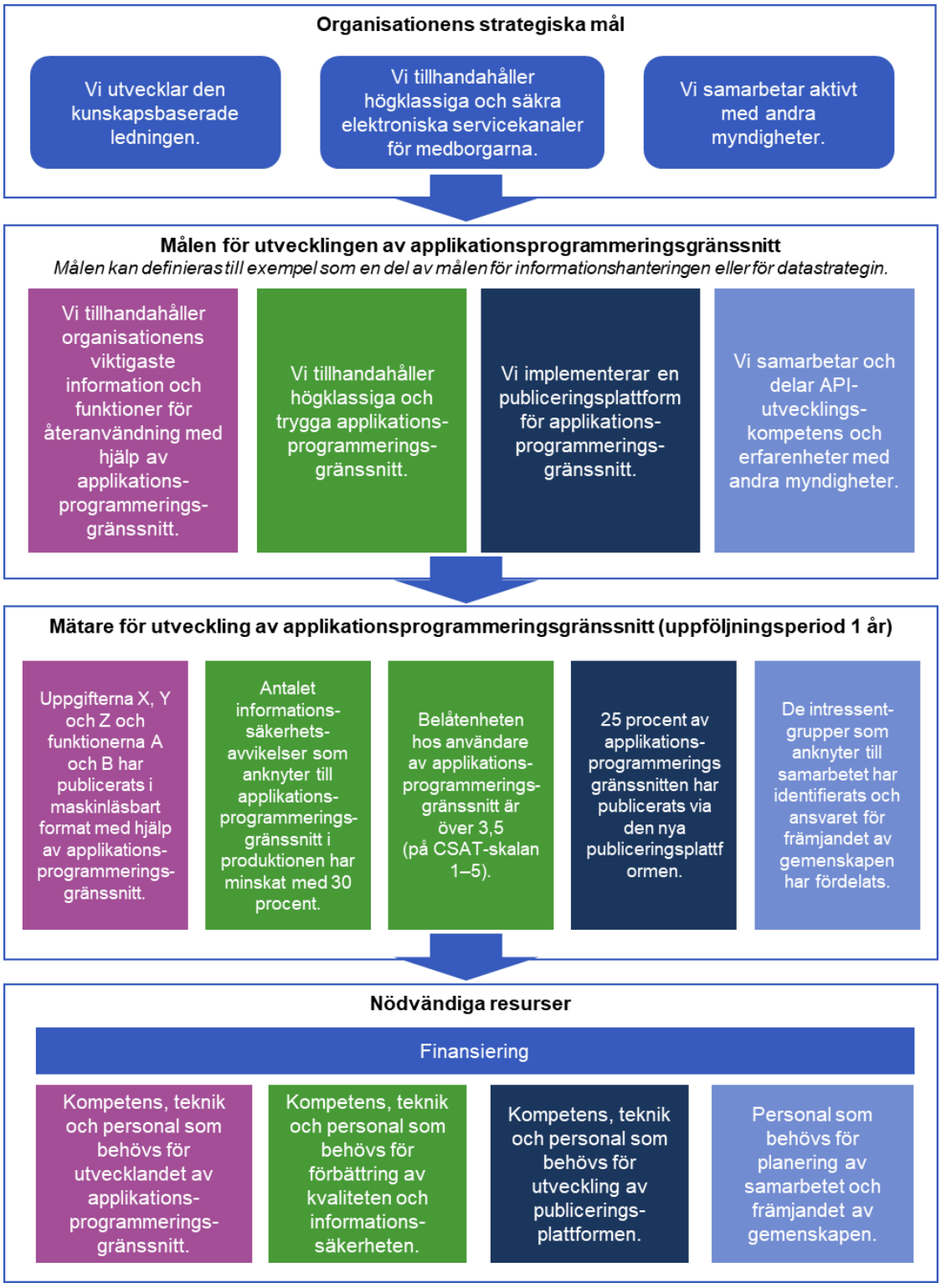

Bild 4 - Exempel på mål, indikatorer och resurser

RESULTAT

- Mål och indikatorer för utvecklingen av applikationsprogrammeringsgränssnitt. Kan vara till exempel en del av målen för informationshanteringen eller av datastrategin eller integrationsstrategin.
- Resursplan för uppnåendet av målen, inklusive personal- och teknikresurserna och finansieringen.

STÖDMATERIAL

Exempel på mål som anknyter till tillhandahållandet och användningen av applikationsprogrammeringsgränssnitt och på hur målen kan ställas i relation till organisationens övriga strategi:

- *Helsingfors stads datastrategi*[27]
- *API-utveckling hos Skatteförvaltningen*[28]
- API som en del av de strategiska målen för projektet Utnyttja och öppna informationen[29].

Princip 1.3 Vid upphandling, säkerställ interoperabiliteten med andra informationssystem

Säkerställ att de informationssystem som upphandlas har egenskaper som gör det möjligt att tillhandahålla och använda information via öppna och teknikoberoende applikationsprogrammeringsgränssnitt. Nödvändiga egenskaper är till exempel:

[27] Helsingfors stads datastrategi, kapitel 5 (Digitaalinen Helsinki, 2021)
[28] Skatteförvaltningens API-utveckling (Verohallinto, 2019)
[29] En länk läggs till senare

- färdiga applikationsprogrammeringsgränssnitt i färdiga programvaror med vilka det är möjligt att tillhandahålla information eller funktioner i systemet för andra system.

- verktyg med vilka det är möjligt att utveckla helt nya applikationsprogrammeringsgränssnitt eller anpassa färdiga applikationsprogrammeringsgränssnitt så att de lämpar sig bättre för ändamålet.

- verktyg med vilka det är möjligt att integrera systemet med färdiga applikationsprogrammeringsgränssnitt som andra system erbjuder.

- licensieringsmodell eller -villkor som gör det möjligt att tillhandahålla, använda och återanvända information och funktioner i systemet internt i organisationen med interna applikationsprogrammeringsgränssnitt (intern API) och externt med externa applikationsprogrammeringsgränssnitt (partner-API, offentlig API).

Vid upphandling av informationssystem **ska kraven som gäller tillhandahållande och användning av information upptas i kravspecifikationerna för det objekt som upphandlas redan i anbudsinfordran**[30].

RESULTAT

❖ Kraven på applikationsprogrammeringsgränssnitt är en del av beskrivningen av upphandlingens objekt.

STÖDMATERIAL

❖ *Webbplatsen för Rådgivningsenheten för offentlig upphandling*[31].

[30] Upphandlingslagen (Laki julkisista hankinnoista ja käyttöoikeussopimuksista 1397/2016, 2016).
[31] Rådgivningsenheten för offentlig upphandling (Julkisten hankintojen neuvontayksikkö, 2021)

Princip 1.4 Främja internt och externt samarbete

Identifiera behoven av internt och externt samarbete som gäller tillhandahållande och användning av applikationsprogrammeringsgränssnitt. Samarbetsbehoven kan gälla till exempel:

- identifiering eller delning av idéer eller behov.
- utveckling eller delning av mål, verksamhetsmodeller, anvisningar eller instruktioner.
- utveckling eller delning av lösningar.
- delning av kunnande eller erfarenheter.

Identifiera de intressentgrupper med vilka samarbete borde göras. Observera att samarbete görs på olika nivåer i organisationer. Intressentgrupper är exempelvis:

- ledningen för den egna organisationen eller någon annan organisation.
- personer eller team som utvecklar informationshanteringen i den egna organisationen eller någon annan organisation.
- teamen för utveckling och administration i den egna organisationen eller någon annan organisation.

Definiera de personer eller team i din egen organisation som borde främja eller delta i samarbetet. Diskutera med dem med vilken samarbetsstruktur ni skulle kunna främja och effektivisera användningen av information internt och externt med hjälp av applikationsprogrammeringsgränssnitt. I små organisationer kan det vara fråga om bara ett par personer, och då är det särskilt viktigt att samarbeta och dela erfarenheter i nätverk.

Definiera och börja använda de nödvändiga samarbetsmetoderna. Ta hänsyn till existerande samarbetsnätverk och -forum.

RESULTAT

- ❖ Plan för samarbetet, inklusive interna och externa intressentgrupper och samarbetsmetoder.
- ❖ Samarbetets resultat, till exempel identifierade behov, delade lösningar eller erfarenheter samt utveckling av kunnandet.

STÖDMATERIAL

Exempel på existerande samarbetsforum:

- *Nätverket för öppen information*[32]
- *Lantmäteriverkets samarbetsgrupper*[33]
- *Nätfakturaforum*[34]
- *Facebookgruppen API-Suomi*[35]
- *Github-gemenskaperna*[36]
- *Finlands Standardiseringsförbund SFS rf:s standardiseringsgrupper för informations- och kommunikationsteknik*[37].

[32]Nätverket för öppen information (Varsinais-Suomen liitto, 2021)
[33]Lantmäteriverkets samarbetsgrupper (Maanmittauslaitos, 2021c)
[34]Nätfakturaforum (TIEKE Tietoyhteiskunna Kehittämiskeskus Ry, 2021)
[35]Facebookgruppen API-Suomi (Honkanen, 2021)
[36] Github-gemenskaperna (GitHub, 2021)
[37] Standardiseringsgrupperna för informations- och kommunikationsteknik (Suomen standardisoimisliitto SFS Ry, 2021b)

3.2 Taktisk nivå

Bild 5 - Principer på taktisk nivå

Princip 2.1 Utveckla applikationsprogrammeringsgränssnitt behovsorienterat

Identifiera de interna och externa intressentgrupper som anknyter till applikationsprogrammeringsgränssnitt och samla in information om behov och krav av dem. Intressentgrupper är exempelvis:

- aktörer som anknyter till värdekedjan, såsom leverantören av en digital nyttighet och applikationsprogrammeringsgränssnittets leverantör eller potentiella användare.

- personer, team eller grupper, ledare, planerare, utvecklare, testare eller administratörer som arbetar med informationshantering i den egna organisationen eller hos någon annan aktör.

Behoven kan anknyta till applikationsprogrammeringsgränssnittens funktionaliteter eller icke-funktionaliteter, såsom till tillgänglighet, användbarhet eller utvecklarupplevelse. Observera också de krav som lagstiftningen medför[38]. Information om behov kan samlas in bland annat med hjälp av enkäter, responskanaler, samarbetsgrupper, verkstäder eller andra samarbetsmetoder. Om det är fråga om ett offentligt applikationsprogrammeringsgränssnitt vars användare inte kan identifieras kan det vara svårt att samla in information om behoven direkt av användarna eller de potentiella användarna. Även i detta fall är det möjligt att lägga ut en öppen responskanal för användarna.

Prioritera och utveckla egenskaper som anknyter till applikationsprogrammeringsgränssnitten utifrån behoven. Observera behoven under applikationsprogrammeringsgränssnittens hela livscykel från behovskartläggningen till urbruktagningen: definiera och planera, konkurrensutsätt och upphandla, genomför och utveckla, ta i bruk, administrera och ta bort egenskaper hos applikationsprogrammeringsgränssnitten efter behoven och kraven.

RESULTAT

❖ En prioriterad lista över behov och utvecklingsobjekt som anknyter till applikationsprogrammeringsgränssnitt, till exempel en arbetskö (backlog).

[38] Till exempel kravet i informationshanteringslagen om regelbundet återkommande och standardiserad elektronisk överföring av information mellan informationssystem via tekniska gränssnitt (Tiedonhallintalaki 906/2019, 2019) samt de krav som ställs i lag på behandlingen av säkerhetsklassificerade handlingar (Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa, 1101/2019). Ta också del av informationshanteringsnämndens rekommendationer (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020-2021).

STÖDMATERIAL

Exempel på öppna respons- och kontaktkanaler som offentliga organisationer lagt ut:

- *Skatteförvaltningens API-observationsformulär*[39]
- *Meteorologiska institutets kontaktformulär för nättjänsterna för öppna data*[40].

Princip 2.2 Definiera rollerna, uppgifterna, ansvaren och verksamhetsmodellerna som anknyter till tillhandahållandet och användningen av applikationsprogrammeringsgränssnitt

Definiera och börja använda rollerna, uppgifterna och ansvaren som anknyter till tillhandahållandet och användningen av applikationsprogrammeringsgränssnitt. Observera uppgifterna som gäller hanteringen av applikationsprogrammeringsgränssnittshelheten såsom administration av informationshanteringsmodellen, riskhantering och arkitekturstyrning samt uppgifterna som gäller tillhandahållandet och användningen av applikationsprogrammeringsgränssnitt. Användning av applikationsprogrammeringsgränssnitt innebär i praktiken integration med ett applikationsprogrammeringsgränssnitt. Applikationsprogrammeringsgränssnitt och integrationer har en livscykel, och därför ska livscykelns olika skeden observeras i uppgifterna:

- kartläggning av behoven som gäller applikationsprogrammeringsgränssnittet eller integrationen
- specifikation och planering av applikationsprogrammeringsgränssnittet eller integrationen
- konkurrensutsättningar och upphandlingar som gäller applikationsprogrammeringsgränssnittet eller integrationen
- genomförande och utveckling av applikationsprogrammeringsgränssnittet eller integrationen

[39] Skatteförvaltningens API (Verohallinto, 2021b)
[40] Meteorologiska institutets öppna data och källkod (Ilmatieteen laitos, 2021)

- ibruktagning av applikationsprogrammeringsgränssnittet eller integrationen
- administration av applikationsprogrammeringsgränssnittet eller integrationen
- urbruktagning av applikationsprogrammeringsgränssnittet eller integrationen.

Definiera och börja använda de verksamhetsmodeller eller processer som behövs för att tillhandahålla och använda applikationsprogrammeringsgränssnitt, till exempel processer för planering, utveckling, testning, publicering och administration.

Bild 5 Visar ett exempel på olika aktörer i API-värdekedjan samt på aktörernas roller, uppgifter och ansvar under beaktande av hanteringen av helheten av applikationsprogrammeringsgränssnitt och tillhandahållandet och användningen av applikationsprogrammeringsgränssnitt. Syftet med exemplet är att åskådliggöra rollerna, uppgifterna och ansvaren. I en stor organisation är det möjligt att fördela uppgifterna till olika personer och team. I en liten organisation kan det hända att enskilda personer får flera av de uppgifter för team eller roller som presenteras på bilden. När verksamhetsmodellerna planeras har organisationens storlek och struktur avgörande betydelse.

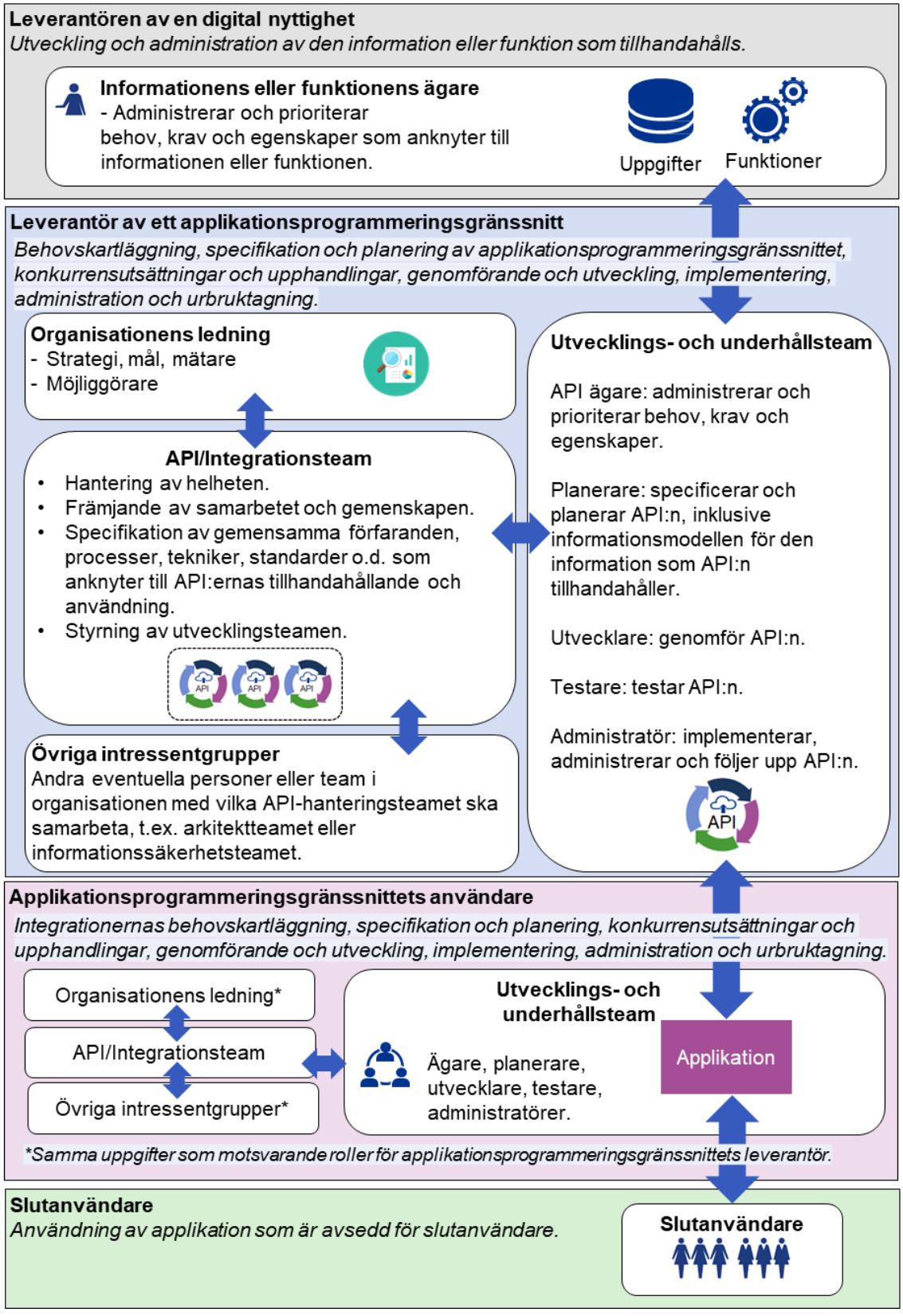

Bild 6 - Exempel på aktörer, roller och ansvar

RESULTAT

- Beskrivning av rollerna, uppgifterna och ansvaren samt ansvarsfördelningen.
- Process- och/eller verksamhetsmodellsbeskrivningar.

STÖDMATERIAL

Exempel på verksamhetsmodeller eller metoder som lämpar sig för utveckling av applikationsprogrammeringsgränssnitt och integrationer:

- *ApiOpsCycles*, som erbjuder en metod och verktyg som kan användas i olika skeden av utvecklingen av applikationsprogrammeringsgränssnitt[41].
- *DevOps (Development and Operation)* som bygger på principerna för agil utveckling, fortlöpande integration, fortlöpande leverans och automatisering[42].
- *DevSecOps (Development, Security and Operation)*, som utvidgar DevOps genom att komplettera den med starkare fokus på informationsssäkerhet i varje skede[43].

Princip 2.3 Beskriv helheten av applikationsprogrammeringsgränssnitt

Definiera och börja använda ett sätt att beskriva helheten av applikationsprogrammeringsgränssnitt. Det är viktigt att kunna hantera de applikationsprogrammeringsgränssnitt som tillhandahålls, för vem och för vilka ändamål applikationsprogrammeringsgränssnitten tillhandahålls samt vilka applikationsprogrammeringsgränssnitt som används, från vem och för vilka ändamål. De applikationsprogrammeringsgränssnitt som tillhandahålls och används kan vara organisationens interna applikationsprogrammeringsgränssnitt (intern API) eller externa applikationsprogrammeringsgränssnitt (partner-API, offentlig API). Tillhandahållarna eller användarna av externa applikationsprogrammeringsgränssnitt kan vara nationella aktörer, till exempel någon annan offentlig eller privat organisation, eller

[41] ApiOpsCycles (APIOps Cycles TM, 2021)
[42] Flera olika källor, bl.a (ite wiki, 2021)och (DevOps.com, 2021)
[43] Flera källor, bl.a. DevSecOps Fundamentals, sid. 17 (Department of Defence, United States of America, 2021) och DevSecOps Manifesto (DevSecOps, 2021)

internationella aktörer, såsom en annan medlemsstat i Europeiska unionen eller en internationell kommersiell organisation.

Observera de olika arkitekturaspekterna och länkningarna till informationshanteringsmodellen i beskrivningarna[44]:

- Med tanke verksamhetsarkitekturen deltar applikationsprogrammeringsgränssnitt i genomförandet av en process eller funktion. Länkningen till en process kan utföras till exempel genom ett informationslager eller informationssystem.

- Med tanke på dataarkitekturen behandlar applikationsprogrammeringsgränssnitt uppgifter i ett eller flera informationslager.

- Med tanke på informationssystemarkitekturen anknyter applikationsprogrammeringsgränssnitt till ett informationssystem.

- Med tanke på den tekniska arkitekturen använder applikationsprogrammeringsgränssnitt en eller flera tekniska resurser.

- Med tanke på integrationsarkitekturen anknyter applikationsprogrammeringsgränssnitt till en eller flera kopplingar, dvs. dataflöden mellan informationssystem.

- Med tanke på informationssäkerhetsarkitekturen orsakar applikationsprogrammeringsgränssnitt risker som ska identifieras och hanteras med hjälp av riskhanteringsåtgärder.

- Med tanke på informationshanteringsmodellen fördjupar beskrivningarna av applikationsprogrammeringsgränssnitt informationshanteringsmodellens beskrivningar[45]. Ur informationshanteringsmodellen är det möjligt att härleda beskrivningarna till den offentliga förvaltningens informationshanteringskarta[46] och beskrivning av handlingarnas offentlighet[47].

Element i applikationsprogrammeringsgränssnitt som ska beskrivas är:

[44] Informationshanteringslagen, 5 § (Tiedonhallintalaki 906/2019, 2019), ta också del av rekommendationen om informationshanteringsmodellen (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:29)
[45]Rekommendation om informationshanteringsmodellen (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:29), ta också del av rekommendationen om tekniska gränssnitt och elektroniska förbindelser (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:21).
[46] Länken saknas, kartan publiceras hösten 2021
[47] Lagen om informationshantering 28 § (Tiedonhallintalaki 906/2019, 2019)

- Beteckning: namn, identifierare eller annan individualiserande uppgift med hjälp av vilken ett applikationsprogrammeringsgränssnitt kan särskiljas från andra applikationsprogrammeringsgränssnitt.

- Ändamål: kortfattad verbal beskrivning av det ändamål för vilket applikationsprogrammeringsgränssnittet används.

- Ägare: Person eller team som ansvarar för applikationsprogrammeringsgränssnittets behov, krav och egenskaper. Till exempel om applikationsprogrammeringsgränssnittet är en del av ett informationssystem kan applikationsprogrammeringsgränssnittets ägare vara samma aktör som informationssystemets ägare. Om applikationsprogrammeringsgränssnittet är en separat, fristående produkt ska det ha en klart definierad ägare.

- Livscykel: en status för livscykeln som beskriver i vilket skede av livscykeln applikationsprogrammeringsgränssnittet är. Statusarna i livscykeln kan härledas ur de olika skedena i applikationsprogrammeringsgränssnittets livscykel som är: specifikation och planering, konkurrensutsättning och upphandling, genomförande och utveckling, ibruktagning, administration, urbruktagning. Som enklast kan statusarna vara till exempel: under utveckling/i användning/kommer att tas ur bruk/har tagits ur bruk.

- Leverantör: den som tillhandahåller applikationsprogrammeringsgränssnittet och ett informationssystem som anknyter till applikationsprogrammeringsgränssnittet, om ett sådant finns.

- Användare: lista över dem som använder applikationsprogrammeringsgränssnittet. Om enskilda användare inte är kända eller identifierade, till exempel om applikationsprogrammeringsgränssnittet är öppet för alla, räcker det med att beskriva för vem applikationsprogrammeringsgränssnittet är avsett.

- Uppgifter som behandlas: om applikationsprogrammeringsgränssnittet behandlar information, relationen till informationen, informationslagret, informationsmaterialet eller informationsgruppen.

- Teknik: beskrivning av vilken teknikresurs applikationsprogrammeringsgränssnittet använder.

Beskrivningarna ska hållas aktuella. Använd automatik för att bilda eller administrera uppgifterna i den mån det är möjligt.

I bilderna 6 och 7 presenteras exempel på beskrivning av applikationsprogrammeringsgränssnitt i leverantörens och användarens perspektiv. I exemplet beaktas Informationshanterings-

nämndens rekommendation om informationshanteringsmodellen[48] som bygger på Informationshanteringslagen[49]. Bilderna är fiktiva och presenteras som exempel även om de bygger på det inkomstregistergränssnitt[50] som Skatteförvaltningen i verkligheten tillhandahåller och som andra aktörer kan använda för att automatiskt anmäla sina löneuppgifter till Skatteförvaltningen.

[48]Rekommendation om informationshanteringsmodellen (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:29)
[49] Lagen om informationshantering 5 § (Tiedonhallintalaki 906/2019, 2019)
[50] Inkomstregistrets tekniska gränssnitt (Verohallinto, 2021a)

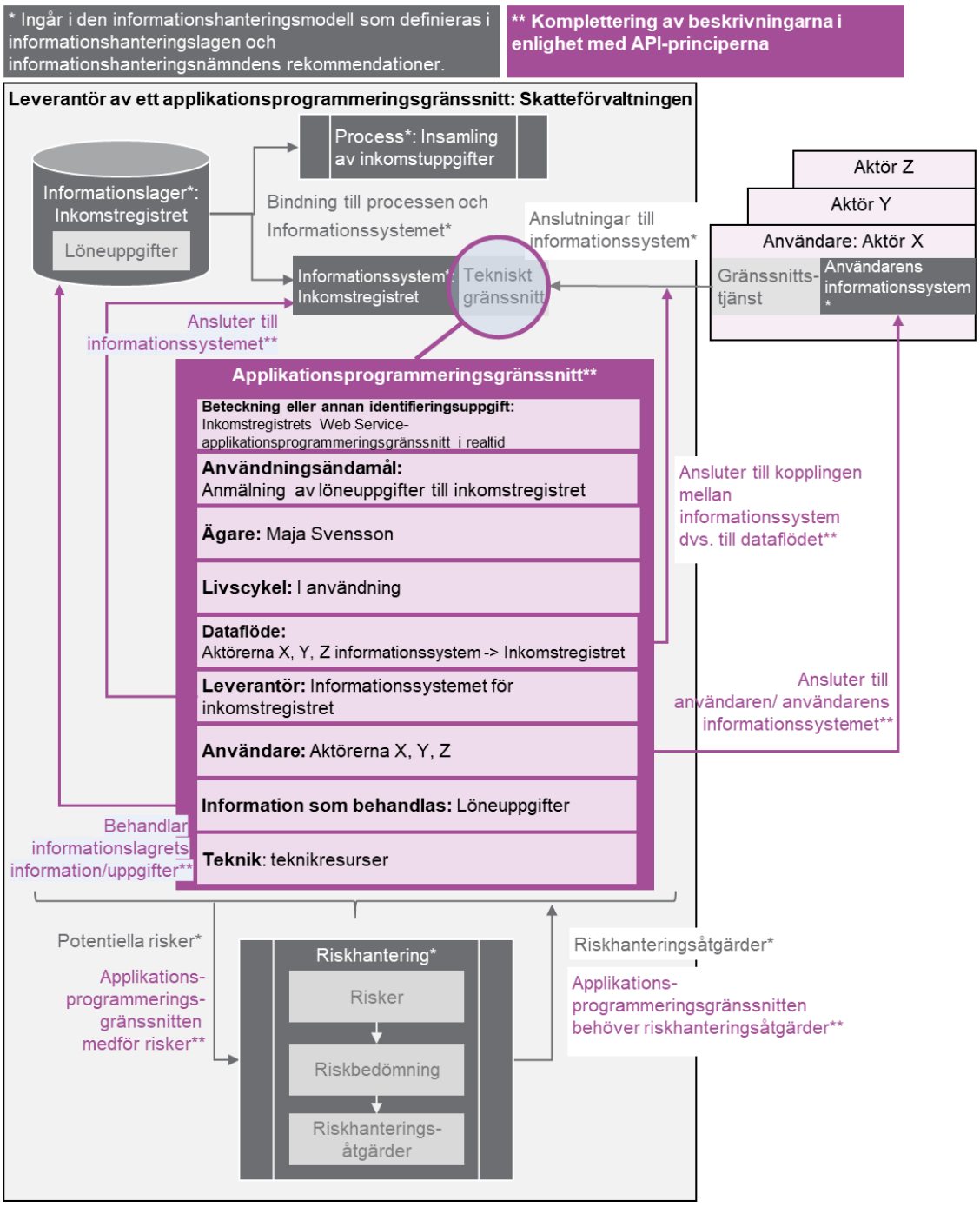

Bild 7 - Rekommendation om beskrivning av applikationsprogrammeringsgränssnitt som en del av informationshanteringsmodellen i applikationsprogrammeringsgränssnittets leverantörs perspektiv

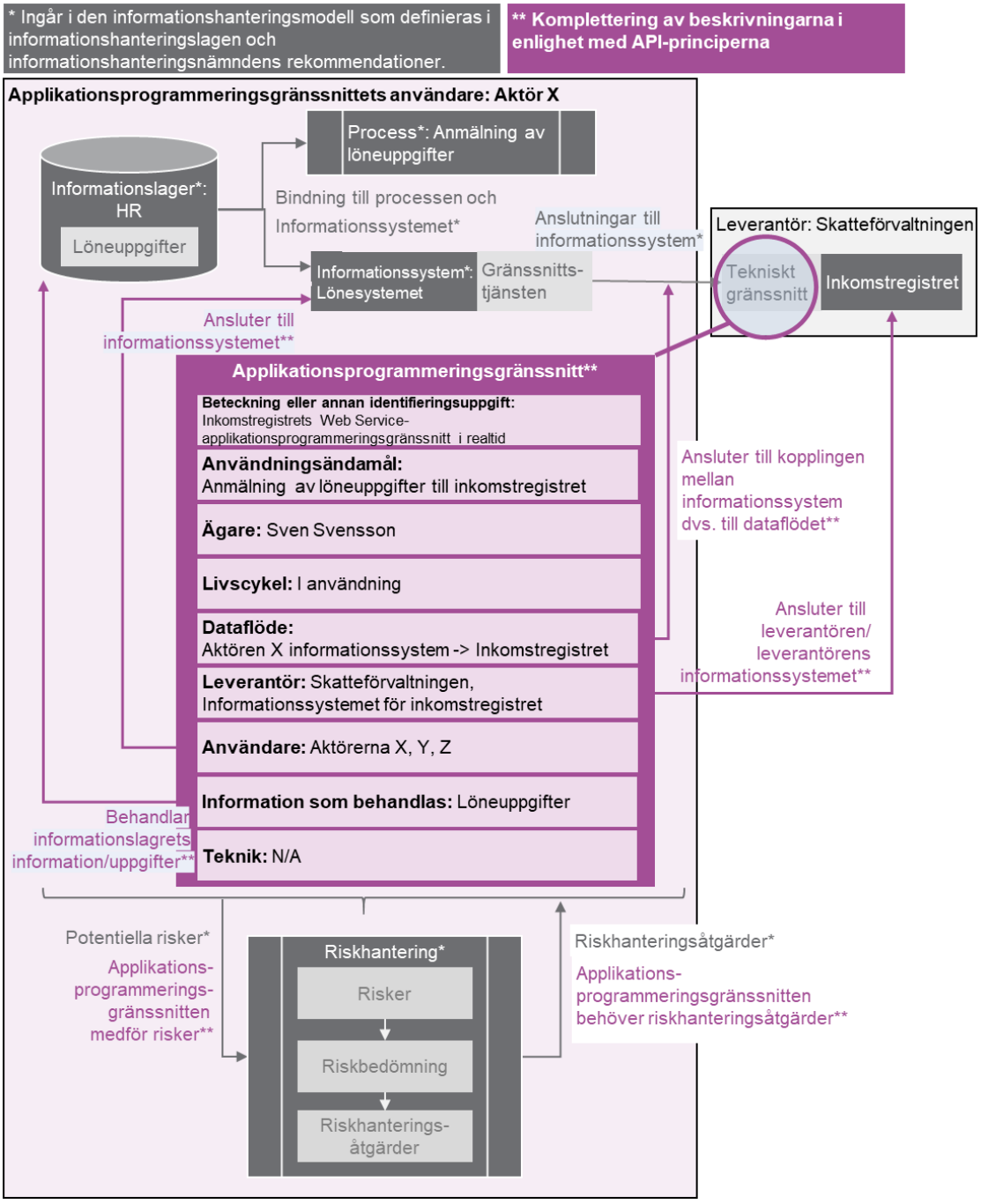

Bild 8 - Rekommendation om beskrivning av applikationsprogrammeringsgränssnitt som en del av informationshanteringsmodellen i applikationsprogrammeringsgränssnittets användares perspektiv

RESULTAT

- Beskrivningar av applikationsprogrammeringsgränssnitt till exempel som en del av informationshanteringsmodellen.

STÖDMATERIAL

- Med hjälp av API-administreringsverktyg är det möjligt att automatiskt samla in information om applikationsprogrammeringsgränssnittens användare. Exempel på API-administrationsverktyg finns bl.a. på *Gartners utvärderingswebbplats*[51].

Ta också del av de följande utbildningarna:

- *Utbildning i eOppiva: Johdanto kokonaisarkkitehtuuriin*[52].
- *Utbildning i eOppiva: Kokonaisarkkitehtuurin mallintaminen*[53].

Princip 2.4 Identifiera och hantera de risker som förknippas med applikationsprogrammeringsgränssnitt

Definiera och börja använda en metod för identifiering av risker och hot som förknippas med applikationsprogrammeringsgränssnitt och för genomförande och uppföljning av riskhanteringsåtgärder. Uppta riskhanteringsåtgärderna i de icke-funktionella kraven på applikationsprogrammeringsgränssnitt.

För riskhantering använd riskhanteringsanvisningen[54] som ledningsgruppen för digital säkerhet VAHTI utarbetat och de riskhanteringsprocesser som redan existerar i din organisation. Riskhanteringsprocessen kan vara till exempel som följer:

[51] Full Life Cycle API Management Reviews and Ratings (Gartner, 2021)
[52] Johdanto kokonaisarkkitehtuuriin (eOppiva, 2021a)
[53] Kokonaisarkkitehtuurin mallintaminen (eOppiva, 2021b)
[54] VAHTI riskhanteringsanvisning (Digi- ja väestötietovirasto, 2021a)

- Välj det applikationsprogrammeringsgränssnitt eller den servicehelhet som bildas av applikationsprogrammeringsgränssnitt som riskhanteringen ska gälla.

- Identifiera de uppgifter som applikationsprogrammeringsgränssnitten behandlar samt uppgifternas klassificering och ägare.

- Identifiera hur kritiska applikationsprogrammeringsgränssnitten är för verksamheten samt de faktorer som anknyter till det, till exempel randvillkor som gäller kontinuitet och återställning.

- Identifiera de hot och risker som förknippas med applikationsprogrammeringsgränssnittet och den information som det behandlar.

- Prioritera kända risker och definiera riskhanteringsåtgärder för dem.

- Definiera ansvaret för genomförandet och uppföljningen av riskhanteringsåtgärderna och andra möjliga fortsatta åtgärder.

Observera också de lagstadgade kraven på behandlingen av information. Vid behandling av säkerhetsklassificerad information iakttas anvisningarna om behandling av säkerhetsklassificerade handlingar[55]. Konfidentiella kommunikationsuppgifter skyddas i enlighet med lagen om tjänster inom elektronisk kommunikation[56] och personuppgifter skyddas i applikationsprogrammeringsgränssnitten i enlighet med dataskyddsförordningen[57] och -lagen[58].

RESULTAT

❖ Ett riskregister som innehåller de risker som applikationsprogrammeringsgränssnitten medför.

❖ Riskhanteringsåtgärder, inklusive hanteringsåtgärder som definierats i syfte att hantera risker som gäller applikationsprogrammeringsgränssnitt.

[55] Rekommendation om behandling av säkerhetsklassificerade handlingar (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:19)
[56] Lag om tjänster inom elektronisk kommunikation (Laki sähköisen viestinnän palveluista 7.11.2014/917, 2014). Ta också del av Cybersäkerhetscentrets webbsida om konfidentiell kommunikation (Kyberturvallisuuskeskus, 2021b)
[57] Den allmänna dataskyddsförordningen (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 2016/679)
[58] Dataskyddslagen (Tietosuojalaki , 5.12.2018/1050)

STÖDMATERIAL

Exempel på de vanligaste riskerna som gäller applikationsprogrammeringsgränssnitt och på åtgärder för hantering av dem:

- *OWASP API Security Top 10*: De vanligaste riskerna som gäller applikationsprogrammeringsgränssnitt och åtgärder för att hantera/förhindra dem[59].

Ta också del av de följande materialen:

- *VAHTI riskhanteringsanvisning*[60]
- *Bilaga 1 exempel på riskhantering av applikationsprogrammeringsgränssnitt med hjälp av informationsriskanalys.*
- Princip 2.3 Bild 7 - Rekommendation om beskrivning av applikationsprogrammeringsgränssnitt som en del av informationshanteringsmodellen i applikationsprogrammeringsgränssnittets leverantörs perspektiv och Bild 8 - Rekommendation om beskrivning av applikationsprogrammeringsgränssnitt som en del av informationshanteringsmodellen i applikationsprogrammeringsgränssnittets användares perspektiv, där riskhantering åskådliggörs som en del av informationshanteringsmodellen.
- *Cybersäkerhetscentrets guide Säker utveckling: med sikte på godkännande*[61].

[59] OWASP API Security Top 10 2019 The ten most critical API security risks (OWASP, 2019)
[60] VAHTI riskhanteringsanvisning (Digi- ja väestötietovirasto, 2021a)
[61] Cybersäkerhetscentrets guide Säker utveckling: med sikte på godkännande (Kyberturvallisuuskeskus, 2020)

3.3 Operativ nivå

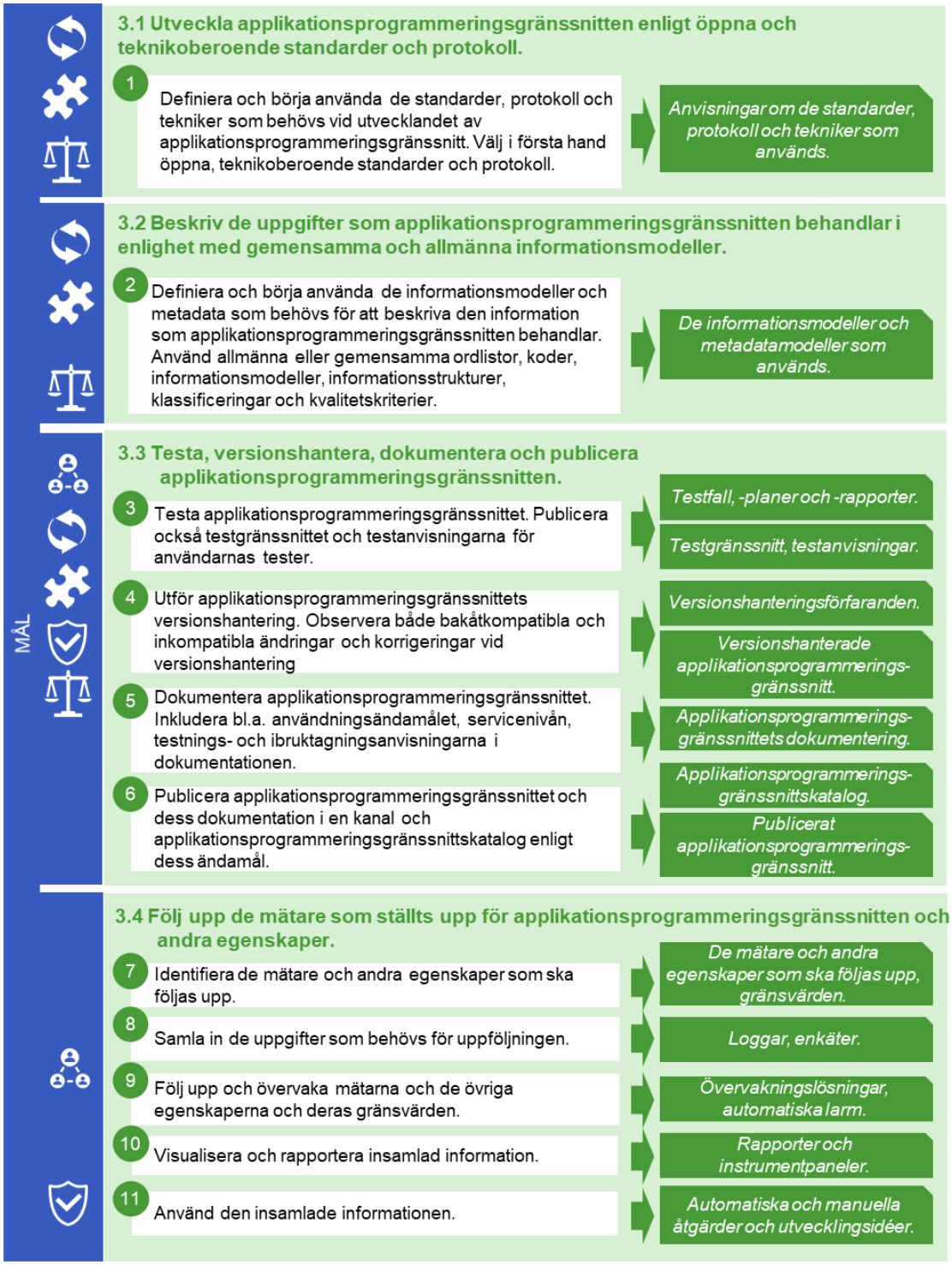

Bild 9 - principerna på operativ nivå

Princip 3.1 Utveckla applikationsprogrammeringsgränssnitten enligt öppna och teknikoberoende standarder och protokoll

Definiera och börja använda de standarder, protokoll och tekniker som behövs vid utvecklandet av applikationsprogrammeringsgränssnitt. För att utveckla applikationsprogrammeringsgränssnitt behövs till exempel:

- ett **dataöverföringsprotokoll** som anger på vilket sätt information kan föras till eller hämtas från applikationsprogrammeringsgränssnittet.

- ett **filformat** som anger i vilket format den information som applikationsprogrammeringsgränssnittet behandlas beskrivs. Filformatet ska vara maskinläsbart. Filformatet kan bygga till exempel på en öppen eller branschspecifik standard eller notation.

- **protokoll och metoder som anknyter till informationssäkerheten** och med vilka det är möjligt att kryptera och kontrollera åtkomsten till information.

- **branschspecifika standarder** som definierar de gemensamma förfaranden som används nationellt eller internationellt i en särskild bransch.

Definiera de dataöverföringsprotokoll, filformat, standarder, protokoll och förfaranden som gäller informationens innehåll eller informationssäkerhet som ska användas de interna och externa applikationsprogrammeringsgränssnitten i din organisation. **Välj i första hand öppna, teknikoberoende standarder och protokoll.** Ta hänsyn till branschspecifika standarder och anvisningar.

Observera att de informationssäkerhetsprotokoll eller -metoder som används ska tillåta utförandet av de åtgärder för informationssäkerhet som riskhanteringen definierat, dvs. de ska väljas utifrån de åtgärder för informationssäkerhet som utsetts. Informationssäkerhetsåtgärderna definieras till exempel utifrån säkerhetsklassificeringen av den information som applikationsprogrammeringsgränssnittet behandlar.

RESULTAT

❖ Organisationen har anvisningar om de standarder, protokoll och tekniker som används vid utvecklandet av applikationsprogrammeringsgränssnitt.

STÖDMATERIAL

Exempel på dataöverföringsprotokoll:

- I webbaserade applikationsprogrammeringsgränssnitt används i allmänhet ett dataöverföringsprotokoll eller en arkitekturmodell som bygger på http, t.ex. *SOAP*[62], *REST (Representational State Transfer)*[63] eller *GraphQL*[64]. Det är rekommenderat att tillhandahålla informationen och funktionerna över webbaserade gränssnitt om detta är möjligt och förenligt med ändamålet. Webbaserade gränssnitt kan användas i både interna och externa gränssnitt, och det är möjligt att implementera en stor mängd informationssäkerhetskontroller i dem.

- I filbaserade applikationsprogrammeringsgränssnitt används i allmänhet ett filbaserat protokoll, t.ex. FTP, SFTP eller FTPS. Även http-baserade protokoll kan användas för att tillhandahålla eller ta emot filer. Filbaserade applikationsprogrammeringsgränssnitt kan användas i både interna och externa gränssnitt. I externa gränssnitt gäller det att implementera tillräckliga informationssäkerhetskontroller. Filbaserade gränssnitt är bra när uppgiften eller funktionen inte behövs i realtid eller då de uppgifter som överförs är i filformat, till exempel bilder, videor eller exceltabeller.

- I databasbaserade applikationsprogrammeringsgränssnitt används vanligen ett databasbaserat protokoll som gör det möjligt att öppna en förbindelse för ett informationssystem, en applikation eller en programvara till databasen och att exekvera operationer gentemot databasen. Databasbaserade applikationsprogrammeringsgränssnitt ska helst användas endast internt i organisationen. Om det är nödvändigt att tillhandahålla uppgifter i ett informationslager till andra aktörer ska till exempel ett webbaserat applikationsprogrammeringsgränssnitt utarbetas mellan informationslagret och den andra aktören.

Exempel på filformat:

- I webbaserade gränssnitt används i allmänhet *XML*[65] eller *JSON*[66]. XML-meddelanden kan beskrivas med ett *XML-schema*[67] och JSON-meddelanden med ett *JSON-schema*[68].

[62] XML Soap (W3Schools, 2021e)
[63] RESTFul Web Services (W3Schools, 2021b)
[64] A query language for your API (GraphQL Foundation, 2021)
[65] XML Tutorial (W3Schools, 2021f)
[66] JSON - Introduction (W3Schools, 2021a)
[67] XML Schema Tutorial (W3Schools, 2021d)
[68] JSON Schema (JSON Schema, 2021)

- I filbaserade gränssnitt kan nästa vilka filformat som helst användas, till exempel bildfiler (.jpg, .gif, .png), videofiler (.mp4, .avi) eller tabeller (.xslx, .csv).

- I databasbaserade gränssnitt är filformatet i allmänhet en struktur som databasen definierar och som kan bygga på en vy, tavla, procedur eller annan databasskript.

Exempel på protokoll och metoder som anknyter till informationssäkerheten:

- I applikationsprogrammeringsgränssnitt krypteras informationen och dataöverföringen oftast med det skyddade överföringsprotokollet *HTTPS*[69] och krypteringsprotokollet *TLS*[70]. I applikationsprogrammeringsgränssnitt som är avsedda för partner kan utöver kryptering också VPN-teknik (Virtual Private Network) användas för att skapa en skyddad tunnel mellan tjänstens leverantör och användare. När säkerhetsklassificerade uppgifter används ska krypteringen uppfylla *Cybersäkerhetscentrets krav på kryptografisk styrka (på finska)*[71].

- I applikationsprogrammeringsgränssnitten kan användas till exempel Basic- eller Bearer-autentisering som http(s)-protokollet möjliggör, autentisering som bygger på API-nyckel, OAuth-protokollet eller från det härledda varianter eller certifikat. Identifieringsmekanismen ska väljas med hjälp av riskbedömning.

- Bekanta dig också *med Cybersäkerhetscentrets anvisningar om elektronisk autentisering*[72] ja och med Myndigheten för digitalisering och befolkningsdata DVV:s *tjänster för identifiering* och *fullmakter*[73].

Exempel på branschspecifika standarder och anvisningar:

- *Standarder och rekommendationer för geodatabranschen*[74]

- *Gränssnittskarta för integrationer och informationssystem inom social- och hälsovården*[75].

- *Nationella och internationella standarder som utarbetats av Finlands Standardiseringsförbund SFS rf:s standardiseringsgrupper*[76]

---

[69] REST Security Cheat Sheet, HTTPS (OWASP Cheat Sheet Series, 2021a)
[70] Transport Layer Protection Cheat Sheet (OWASP Cheat Sheet Series, 2021b)
[71]Cybersäkerhetscentrets krav på kryptografisk styrka (Kyberturvallisuuskeskus, 2021a)
[72] Cybersäkerhetscentret, elektronisk identifiering (Kyberturvallisuuskeskus, 2021c)
[73] Tjänsterna för identifiering och fullmakter (Digi- ja väestötietovirasto, 2021c), (Digi- ja väestötietovirasto, 2021d)
[74] Standarder och rekommendationer för geodatabranschen (Maanmittauslaitos, 2021a)
[75] Gränssnittskarta (HL7 Finland, 2021)
[76] Standardiseringsgrupper (Suomen standardisoimisliitto SFS Ry, 2021a)

Princip 3.2 Beskriv de uppgifter som applikationsprogrammeringsgränssnitten behandlar i enlighet med gemensamma och allmänna informationsmodeller

Definiera och börja använda de informationsmodeller och metadata som behövs för att beskriva den information som applikationsprogrammeringsgränssnitten behandlar. Använd allmänna eller gemensamma ordlistor, koder, informationsmodeller, informationsstrukturer, klassificeringar och kvalitetskriterier[77]. Enligt informationshanteringsnämndens rekommendation ska de ordlistor som används bygga på begrepp som definieras i lag, och de borde inte definieras på nytt med annan betydelse eller annat innehåll. Definitionen av ordlistorna påverkas av 2.3 § i grundlagen, som föreskriver att lag ska noggrant iakttas all offentlig verksamhet. De i lag föreskrivna begreppen är bindande för användningen i myndigheternas verksamhet[78].

RESULTAT

- De informationsmodeller och metadatamodeller som används.

STÖDMATERIAL

Exempel på gemensamma och allmänna ordlistor, koder, informationsmodeller och kvalitetskriterier:

- *Interoperabilitetsplattformen och interoperabilitetsmetoden (på finska)*[79]
- *Statistikcentralens kvalitetskriterier och mätare för information*[80].

Ta också del av de följande materialen:

[77] Informationshanteringsnämndens rekommendation om tekniska gränssnitt och elektroniska förbindelser, sid. 11 (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:21)
[78] Mer information om Informationshanteringsnämndens rekommendation om tekniska gränssnitt och elektroniska förbindelser (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:21)
[79]Interoperabilitetsplattformen och interoperabilitetsmetoden (på finska) (Digi- ja väestötietovirasto, 2021e)
[80]Kvalitetskriterier och kvalitetsmätare för datamaterial (Tilastokeskus, 2021)

❖ *Kommunförbundets video om interoperabilitet i kommunerna*[81].

Princip 3.3 Testa, versionshantera, dokumentera och publicera applikationsprogrammeringsgränssnitten

Testa applikationsprogrammeringsgränssnittet. För testning av applikationsprogrammeringsgränssnittet definiera testfall med vilka det är möjligt att testa funktionella och icke-funktionella krav, t.ex. användbarhet, feltolerans, informationssäkerhet och prestanda. Ta hänsyn till testningens olika skeden: enhets-, integrations-, system- och godkännandetestning samt regressionstestning. Använd testningsautomatisering i den mån det är möjligt. **Publicera också en avgiftsfri testversion av applikationsprogrammeringsgränssnittet och testningsanvisningar, så att användarna kan utföra tester.**

Utför applikationsprogrammeringsgränssnittets versionshantering. Vid versionshanteringen observera publiceringen både av bakåtkompatibla och av inkompatibla ändringar och korrigeringar. Stöd flera gränssnittsversioner samtidigt efter eventuella behov.

Dokumentera applikationsprogrammeringsgränssnittet. I dokumenteringen inkludera:

- applikationsprogrammeringsgränssnittets användningsändamål.
- licensiering av applikationsprogrammeringsgränssnittet och de uppgifter och funktioner som det tillhandahåller.
- applikationsprogrammeringsgränssnittets läge.
- applikationsprogrammeringsgränssnittets servicenivå eller -löfte. Berätta om det inte finns någon servicenivå eller något löfte, till exempel om applikationsprogrammeringsgränssnittet är i försöksstadiet.
- anvisningar för testning och implementering av applikationsprogrammeringsgränssnittet.
- de operationer eller metoder som applikationsprogrammeringsgränssnittet tillhandahåller.
- meddelanden om begäran (request) och svar (respons) som gäller applikationsprogrammeringsgränssnittets operationer eller metoder.

[81] Video om interoperabilitet i kommunerna (Kuntaliitto, 2021)

- eventuella felkoder som applikationsprogrammeringsgränssnittets operationer eller metoder returnerar och deras förklaringar.

I den omfattning det är möjligt, använd redskap som genererar åtminstone en del av dokumentationen automatiskt. Uppta dokumentering till exempel som en del av applikationsprogrammeringsgränssnittets metadata.

Publicera applikationsprogrammeringsgränssnittet och dess dokumentation i en kanal och applikationsprogrammeringsgränssnittskatalog enligt dess ändamål. Publiceringsgränssnittet beror på applikationsprogrammeringsgränssnittets typ (intern, partner eller offentlig API), applikationsprogrammeringsgränssnittets användare och klassificeringen av den information som applikationsprogrammeringsgränssnittet behandlar.

RESULTAT

- ❖ Testfall, testplaner och testrapporter.
- ❖ Testgränssnitt och testanvisningar.
- ❖ Versionshanteringsprinciper och versionshanterade applikationsprogrammeringsgränssnitt.
- ❖ Gränssnittens dokumentationer.
- ❖ Gränssnittets uppgifter i gränssnittskatalogen.
- ❖ Publicerat gränssnitt i publiceringskanalen.

STÖDMATERIAL

Exempel på väldokumenterade gränssnitt, i vilka också användarnas tester möjliggjorts:

- ❖ *Traficom Avoin Data API*[82].

[82] Traficom Avoin Data API (Traficom, 2021)

- *Vero API*[83].

Tilläggsmaterial som gäller testning:

- *Anvisning för testning av API:er* , innehåller också exempel på verktyg som används vid testning av applikationsprogrammeringsgränssnitt[84].
- Övriga systemtestningsanvisningar, såsom *w3chools Software Testing Tutorial Library*[85] eller *Software Testing Fundamentals*[86].
- *DevOps testanvisning av DevOps Institute*[87]*.*

Tilläggsmaterial som gäller versionshantering:

- *Semantisk versionshantering*[88].

Tilläggsmaterial som gäller dokumentering:

- Ta del av *Open API Initiatives Open API Specification*[89] och *RAML*[90] specifikationer.
- De flesta API-administrationsverktyg kommer med automatisk API-dokumentering. Det lönar sig att använda funktionen. Exempel på API-administrationsverktyg finns bl.a. *på Gartners utvärderingswebbplats*[91]. Det finns också separata verktyg, till exempel *Swagger U I* [92].

Exempel på publiceringskanaler för offentliga applikationsprogrammeringsgränssnitt:

- Servicedatalagret eller avoindata.fi[93].

Exempel på publiceringskanaler för applikationsprogrammeringsgränssnitt som är avsedda för partner:

---

[83] Vero API (Verohallinto, 2021b)
[84] A Comprehensive API Testing Guide (Software Testing Materials, 2020)
[85] Software Testing Tutorial Library (W3Schools, 2021c)
[86] Sotware Testing Fundamentals (Software Testing Fundamentals, 2021)
[87] DevOps Testing (Hornbeek, 2021)
[88] Semantic Versioning 2.0.0 (Preston-Werner, 2021)
[89] Open API Specification (Open API Initiative, 2021)
[90] The simplest way to model APIs (RAML, 2021)
[91] Full Life Cycle API Management Reviews and Ratings (Gartner, 2021)
[92] Swagger UI (Swagger, 2021)
[93] En länk läggs till senare

- *Informationsleden Suomi.fi* [94] enligt den *användningsskyldighet*[95] som föreskrivs i lag.
- *Integrationsplattformen VIA* för informationsutbyte mellan statliga organisationer[96].
- Applikationsprogrammeringsgränssnitt som behandlar säkerhetsklassificerad information publiceras i en *nätslusslösning*[97] som uppfyller kraven för den aktuella klassificeringen och dokumentationen som anknyter till dem förvaras på ett *lagringsställe*[98] som uppfyller kraven för den aktuella klassificeringen.
- Dessutom kan det finnas bransch- eller organisationsspecifika publiceringskanaler.

Exempel på publiceringskanaler för interna applikationsprogrammeringsgränssnitt:

- Intern publiceringskanal som organisationen definierat själv. Publiceringskanalen kan vara en *API-Gateway*[99] av något slag eller en annan produkt eller en lösning som organisationen utvecklat själv via vilken de interna applikationsprogrammeringsgränssnitten kan hittas och användas.

Princip 3.4 Följ upp de mätare som ställts upp för applikationsprogrammeringsgränssnitten och andra egenskaper

1. **Identifiera de mätare och andra egenskaper som ska följas upp.** Mätare som ska följas upp är till exempel mätare som specificerats på strategisk nivå. Andra egenskaper som följs upp är egenskaper som är väsentliga med tanke på applikationsprogrammeringsgränssnittens funktion, till exempel huruvida applikationsprogrammeringsgränssnittet är aktiverat eller om CPU-resurserna är tillräckliga. Definiera tillåtna gränsvärden för mätarna och de egenskaper som ska följas upp.

2. **Samla in de uppgifter som behövs för uppföljningen.** Uppgifter kan samlas in till exempel med hjälp av loggar och enkäter av olika slag.

[94] Informationsleden Suomi.fi (Digi- ja väestötietovirasto, 2021b)
[95] Lagen om förvaltningens gemensamma stödtjänster för e-tjänster 3§, 5§ (Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista, 571/2016)
[96] Valtoris integrationstjänster (Valtori, 2021)
[97] Nätslussanvisning (Kyberturvallisuuskeskus, 2018)
[98] Rekommendation om behandling av säkerhetsklassificerad information (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:19)
[99] Full Life Cycle API Management Reviews and Ratings. (Gartner, 2021)

3. **Följ upp och övervaka mätarna och de övriga egenskaperna och deras gränsvärden.** Övervakning kan göras till exempel automatiskt med olika slags övervaknings- eller uppföljningslösningar, eller manuellt med hjälp av rapporter som genereras med regelbundna intervaller. Många övervakningslösningar innehåller också en funktionalitet som gör det möjligt att ställa in automatiska larm när ett gränsvärde över- eller underskrids.

4. **Visualisera och rapportera insamlad information**. Visualisering kan exempelvis göras med hjälp av olika uppföljnings- eller övervakningsverktyg eller med rapporteringslösningar eller rapporter.

5. **Använd den insamlade informationen för att identifiera och vidta nödvändiga åtgärder samt för att utveckla eller ta ur bruk applikationsprogrammeringsgränssnitt.** Vidta de nödvändiga åtgärderna, till exempel återställ ett applikationsprogrammeringsgränssnitt när det ligger nere eller skala applikationsprogrammeringsgränssnittet upp eller ned efter de resurser som det använder (t.ex. CPU eller minne). Använd automatisering i åtgärderna i den mån det är möjligt. Identifiera punkter som kräver utveckling i applikationsprogrammeringsgränssnitten eller anknytande egenskaper. Registrera utvecklingsobjekten i en adekvat arbetskö för prioritering och utveckling. Utvecklingsobjekten kan anknyta till applikationsprogrammeringsgränssnittens funktionaliteter eller icke-funktionaliteter, såsom till deras prestanda eller informationssäkerhet eller till utvecklarupplevelsen.

I bild 10 åskådliggörs de uppgifter som anknyter till uppföljningen av applikationsprogrammeringsgränssnitt och exempel på olika ämnen.

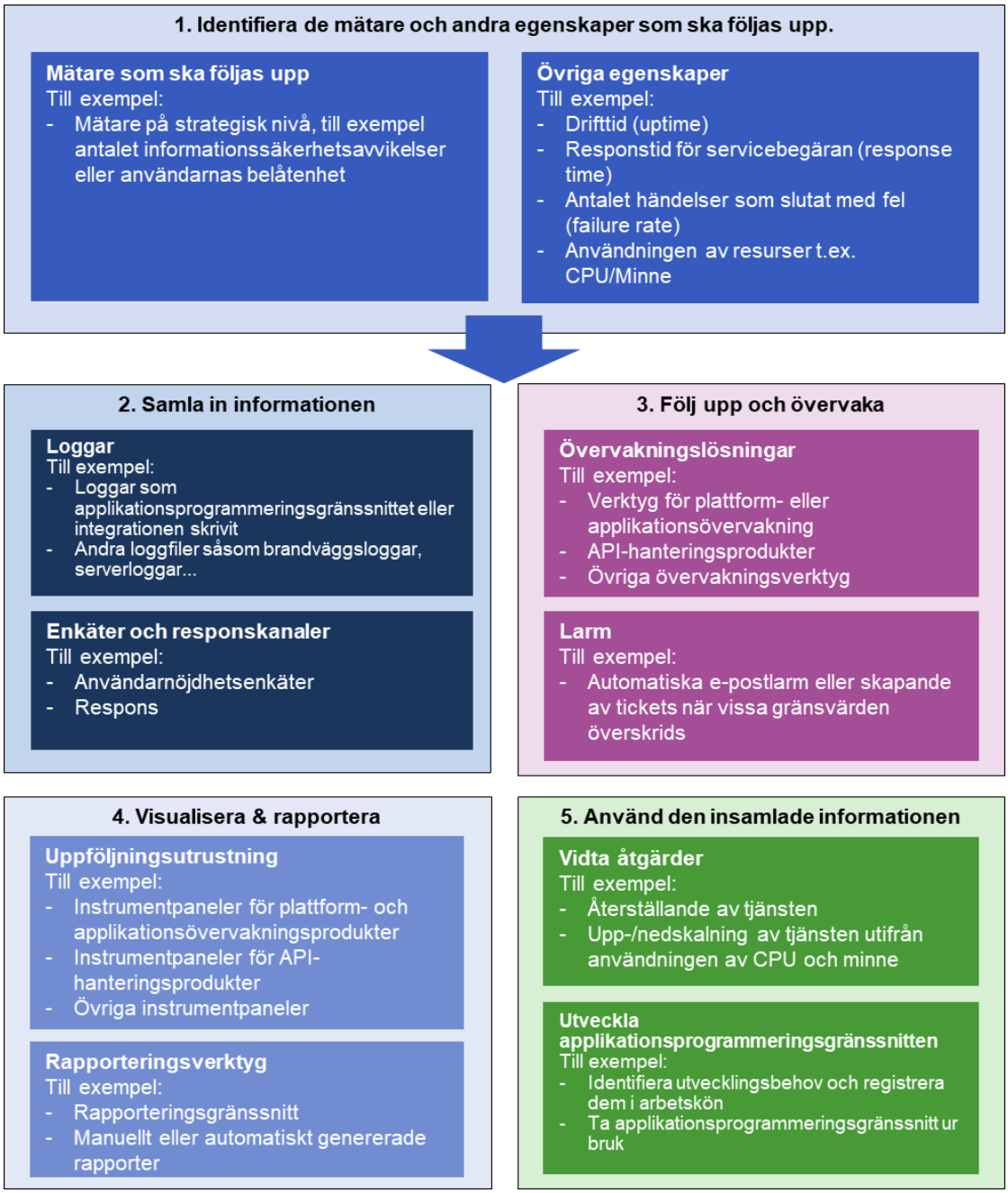

Bild 10 - Uppföljning av applikationsprogrammeringsgränssnitt

RESULTAT

- En lista över mätare och andra egenskaper som ska följas upp jämte gränsvärden.
- Applikationsprogrammeringsgränssnittens och integrationernas loggfiler, övriga loggfiler såsom server- eller brandväggsloggar.
- Enkäter, responskanaler.
- Lösningar för uppföljning och övervakning.
- Automatiska larm.
- Olika instrumentpaneler eller rapporter.
- Åtgärder som ska vidtas automatiskt eller manuellt samt anvisningar om åtgärderna.
- Utvecklingsidéer/utvecklingsbehov, inkl. behovet att ta ett applikationsprogrammerings-gränssnitt ur bruk.

3.4 Sammanfattning av principerna

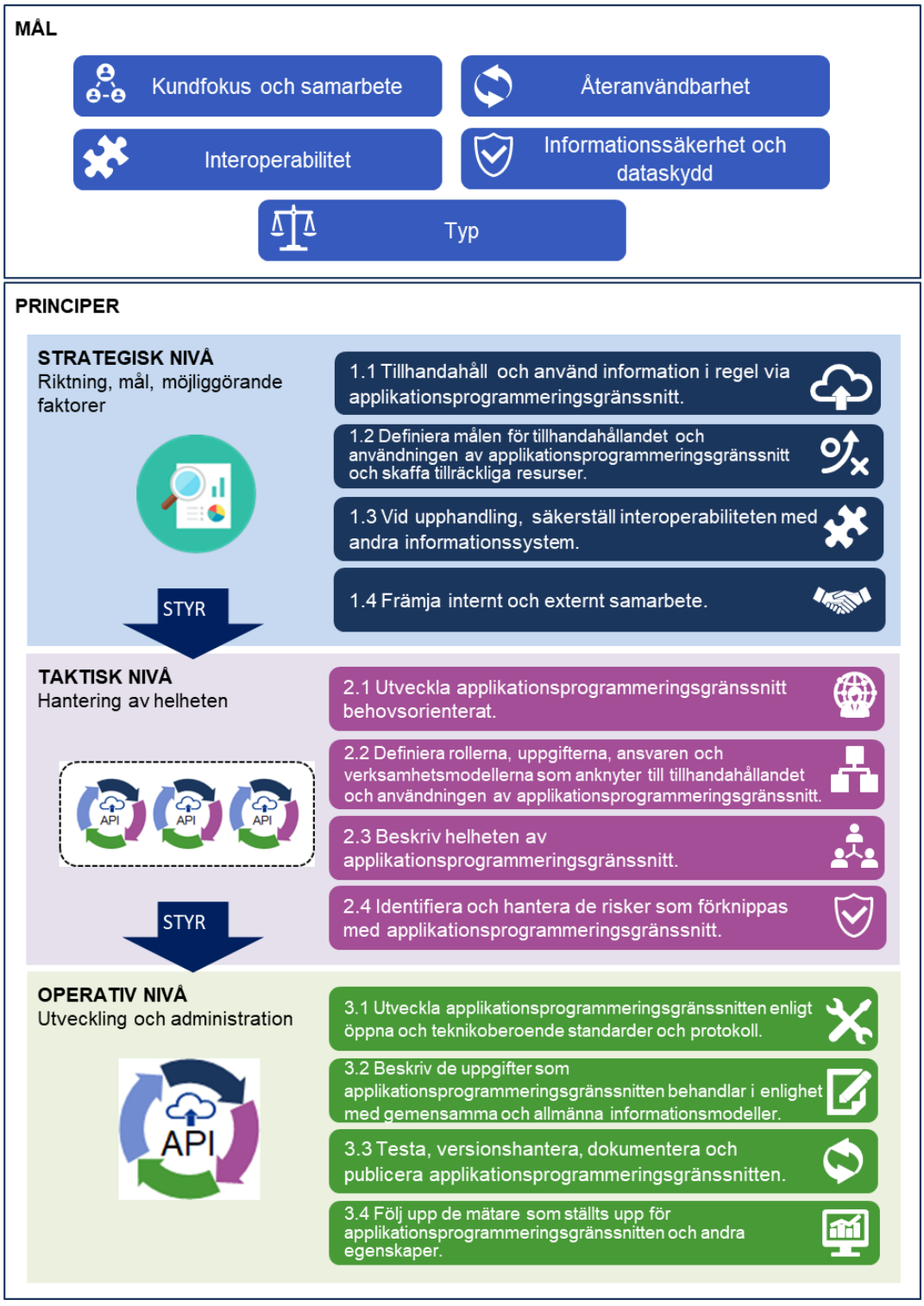

Bild 11 - Sammanfattning av principerna

Källor

Preston-Werner, Tom. 2021. Semantic Versioning 2.0.0. [Online] 2021. [Citat: den 21 6 2021.] https://semver.org/.
APIOps Cycles TM. 2021. APIOps Cycles for Lean API Development. [Online] 2021. [Citat: den 16 6 2021.] https://www.apiopscycles.com/ .
Department of Defence, United States of America. 2021. DoD Enterprise DevSecOps Fundamentals. [Online] 2021. [Citat: den 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. [Citat: den 23 8 2021.] https://devops.com/.
DevSecOps. 2021. Manifesto. [Online] 2021. [Citat: den 5 8 2021.] https://www.devsecops.org/.
Digi- ja väestötietovirasto. 2021a. Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI. [Online] 2021a. [Citat: den 21 6 2021.] https://dvv.fi/vahti.
—. 2021b. Suomi.fi-palveluväylä. [Online] 2021b. [Citat: den 23 8 2021.] https://www.suomi.fi/palvelut/suomi-fi-palveluvayla-digi-ja-vaestotietovirasto/4ab88971-b9fb-443c-99aa-bc361bac7548.
—. 2021c. Tunnistus. [Online] 2021c. [Citat: den 5 8 2021.] https://dvv.fi/tunnistus.
—. 2021d. Valtuudet. [Online] 2021d. [Citat: den 5 8 2021.] https://dvv.fi/valtuudet.
—. 2021e. Yhteentoimivuusalusta. [Online] 2021e. [Citat: den 21 6 2021.] https://dvv.fi/yhteentoimivuusalusta.
Digitaalinen Helsinki. 2021. Helsingin datastrategia. [Online] 2021. [Citat: den 17 6 2021.] https://digi.hel.fi/esittely/helsinki-datastrategia/.
eOppiva. 2021a. Johdanto kokonaisarkkitehtuuriin. [Online] 2021a. [Citat: den 21 6 2021.] https://www.eoppiva.fi/kurssit/johdanto-kokonaisarkkitehtuuriin/#/.
—. 2021b. Kokonaisarkkitehtuurin mallintaminen. [Online] 2021b. [Citat: den 21 6 2021.] https://www.eoppiva.fi/kurssit/kokonaisarkkitehtuurin-mallintaminen/#/.
Euroopan Komissio. 2017. Eurooppalaiset yhteentoimivuusperiaatteet – täytäntöönpanostrategia. [Online] 2017. [Citat: den 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. [Citat: den 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. [Citat: den 23 8 2021.] https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A32007L0002.
Gartner. 2021. Full Life Cycle API Management Reviews and Ratings. [Online] 2021. [Citat: den 21 6 2021.] https://www.gartner.com/reviews/market/full-life-cycle-api-management.
GitHub. 2021. GitHub. [Online] 2021. [Citat: den 30 6 2021.] https://github.com/.
GraphQL Foundation. 2021. A query language for your API. [Online] 2021. [Citat: den 21 6 2021.] https://graphql.org/.
HL7 Finland. 2021. Rajapintakartta. [Online] 2021. [Citat: den 5 8 2021.] http://www.hl7.fi/hl7-rajapintakartta/.
Honkanen, Mika. 2021. API-Suomi. [Online] 2021. [Citat: den 30 6 2021.] https://fi-fi.facebook.com/groups/apisuomi/.
Hornbeek, Marc. 2021. DevOps Testing. [Online] 2021. [Citat: den 30 6 2021.] https://devopsinstitute.com/wp-content/uploads/2018/03/DevOps-testing-ebook-online.pdf.
Ilmatieteen laitos. 2021. Ilmatieteen laitoksen avoin data ja lähdekoodi. [Online] 2021. [Citat: den 16 6 2021.] https://www.ilmatieteenlaitos.fi/avoin-data.

ite wiki. 2021. DevOps. [Online] 2021. [Citat: den 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. [Citat: den 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. [Citat: den 21 6 2021.] https://json-schema.org/.
Julkisten hankintojen neuvontayksikkö. 2021. Julkisten hankintojen neuvontayksikkö. [Online] 2021. [Citat: den 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.
Kuntaliitto. 2021. Yhteentoimivuustyö kunnissa. [Online] 2021. [Citat: den 21 6 2021.] https://www.youtube.com/watch?v=FNNL8K0EBCI.
Kyberturvallisuuskeskus. 2021a. Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat. [Online] 2021a. [Citat: den 1 7 2021.] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf.
—. 2021b. Luottamuksellinen viestintä. [Online] 2021b. [Citat: den 25 8 2021.] https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/luottamuksellinen-viestinta.
—. 2018. Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista. [Online] 2018. [Citat: den 21 6 2021.] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Yhdyskaytavaratkaisuohje.pdf.
—. 2021c. Sähköinen tunnistaminen. [Online] 2021c. [Citat: den 1 7 2021.] https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen.
—. 2020. Turvallinen tuotekehitys - kohti hyväksyntää. [Online] 2020. [Citat: den 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. [Citat: den 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. [Citat: den 23 8 2021.] https://www.finlex.fi/fi/laki/alkup/2016/20161397.
Laki paikkatietoinfrastruktuurista 421/2009. 2009. Laki paikkatietoinfrastruktuurista. [Online] 2009. [Citat: den 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. [Citat: den 25 8 2021.] https://www.finlex.fi/fi/laki/ajantasa/2014/20140917.
Maanmittauslaitos. 2021a. Paikkatietoalan standardit ja suositukset. [Online] 2021a. [Citat: den 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. [Citat: den 30 6 2021.] https://www.maanmittauslaitos.fi/tietoa-maanmittauslaitoksesta/organisaatio/yhteistyoryhmat.
OECD. 2002. Glossary of statistical terms: Quality - ISO. [Online] 2002. [Citat: den 9 6 2021.] https://stats.oecd.org/glossary/detail.asp?ID=5150.
Open API Initiative. 2021. Open API. [Online] 2021. [Citat: den 21 6 2021.] https://www.openapis.org.

OWASP Cheat Sheet Series. 2021a. REST Security Cheat Sheet. [Online] 2021a. [Citat: den 5 8 2021.] https://cheatsheetseries.owasp.org/cheatsheets/REST_Security_Cheat_Sheet.html#https.
—. 2021b. Transport Layer Protection Cheat Sheet. [Online] 2021b. [Citat: den 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. [Citat: den 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. [Citat: den 1 7 2021.] https://raml.org/.
Software Testing Fundamentals. 2021. Sotware Testing Fundamentals. [Online] 2021. [Citat: den 30 6 2021.] https://softwaretestingfundamentals.com/.
Software Testing Materials. 2020. A Comprehensive API Testing Guide. [Online] 2020. [Citat: den 30 6 2021.] https://www.softwaretestingmaterial.com/api-testing/.
Suomen standardisoimisliitto SFS Ry. 2021a. Standardisointiryhmät. [Online] 2021a. [Citat: den 23 8 2021.] https://sfs.fi/osallistu-ja-vaikuta/standardisointiryhmat/?fwp_aihealueet=tieto-ja-viestintatekniikka.
—. 2021b. Tieto- ja viestintätekniikka. [Online] 2021b. [Citat: den 23 8 2021.] https://sfs.fi/osallistu-ja-vaikuta/aihealueet/tieto-ja-viestintatekniikka/.
Swagger. 2021. Swagger UI. [Online] 2021. [Citat: den 21 6 2021.] https://swagger.io/tools/swagger-ui/.
Tiedonhallintalaki 906/2019. 2019. Laki julkisen hallinnon tiedonhallinnasta. [Online] 2019. [Citat: den 8 6 2021.] https://www.finlex.fi/fi/laki/alkup/2019/20190906.
TIEKE Tietoyhteiskunna Kehittämiskeskus Ry. 2021. Verkkolaskufoorumi. [Online] 2021. [Citat: den 30 6 2021.] https://tieke.fi/palvelut/liiketoimintapalvelut/verkkolaskufoorumi/.
Tietosuojalaki . 5.12.2018/1050. Tietosuojalaki. [Online] 5.12.2018/1050. [Citat: den 9 6 2021.] https://www.finlex.fi/fi/laki/ajantasa/2018/20181050.
Tietosuojavaltuutetun toimisto. 2021. Pseudonymisoidut ja anonymisoidut tiedot. [Online] 2021. [Citat: den 25 8 2021.] https://tietosuoja.fi/pseudonymisointi-anonymisointi.
Tilastokeskus. 2021. Tietoaineistojen laatukriteerit. [Online] 2021. [Citat: den 21 6 2021.] https://www.stat.fi/org/vuosiohjelma/tietoaineistojen-laatukriteerit.html.
Traficom. 2021. Traficom Avoin Data API. [Online] 2021. [Citat: den 21 6 2021.] https://opendata.traficom.fi/swagger/ui/index.
Vaccari, L, o.a. 2020. Application Programming Interfaces in Governments: Why, what and how. [Online] 2020. [Citat: den 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. [Citat: den 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. [Citat: den 30 6 2021.] https://finlex.fi/fi/laki/alkup/2019/20191101.
Valtiovarainministeriö. 2021a. Tiedon hyödyntäminen ja avaamisen hanke. [Online] 2021a. [Citat: den 8 6 2021.] https://vm.fi/tiedon-hyodyntaminen-ja-avaaminen1.
—. 2021b. Tiedon hyödyntämisen ja avaamisen kansalliset strategiset tavoitteet. [Online] 2021b. URL PUUTTUU.
—. 2021c. Tiedon yhteentoimivuus. [Online] 2021c. [Citat: den 9 6 2021.] https://vm.fi/tiedon-yhteentoimivuus.
Valtiovarainministeriö, Tiedonhallintalautakunta. 2021:21. Suositus teknisistä rajapinnoista ja katseluyhteyksistä. [Online] 2021:21. [Citat: den 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. [Citat: den 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. [Citat: den 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. [Citat: den 8 6 2021.] https://vm.fi/suositukset.
—. 2020:61. Valtiovarainministeriön julkaisuja – 2020:61 Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta. [Online] 2020:61. [Citat: den 8 6 2021.] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162433/VM_2020_61.pdf?sequence=4&isAllowed=y.. ISBN PDF: 978-952-367-295-6.
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. [Citat: den 21 6 2021.] https://valtori.fi/integraatiopalvelut.
Varsinais-Suomen liitto. 2021. Avoimen tiedon verkosto. [Online] 2021. [Citat: den 30 6 2021.] https://kumppanuusfoorumi.fi/foorumi/avoimen-tiedon-verkosto/.
Väylävirasto. 2021. Väyläviraston avoimet rajapinnat. [Online] 2021. [Citat: den 8 6 2021.] https://vayla.fi/vaylista/aineistot/avoindata/rajapinnat.
Verohallinto. 2019. API-kehittäminen Verolla. [Online] 2019. [Citat: den 17 6 2021.] http://131.207.14.19/contentassets/5389e8bf012445db8fb5865ad0fe745e/10.-api-kehitt%C3%A4minen_verolla.pdf.
—. 2021a. Tulorekisterin tekninen rajapinta. [Online] 2021a. [Citat: den 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. [Citat: den 8 6 2021.] https://avoinomavero.vero.fi/_/.
—. 2021d. Veronumerorekisteri. [Online] 2021d. https://www.suomi.fi/palvelut/veronumerorekisteri-verohallinto/57063087-94c6-4c6e-9e2e-545bb5128010.
W3Schools. 2021a. JSON - Introduction. [Online] 2021a. [Citat: den 21 6 2021.] https://www.w3schools.com/js/js_json_intro.asp.
—. 2021b. RESTful Web services. [Online] 2021b. [Citat: den 21 6 2021.] REST https://www.w3schools.in/restful-web-services/intro/.
—. 2021c. Software Testing Tutorial Library. [Online] 2021c. [Citat: den 30 6 2021.] https://www.w3schools.in/software-testing/.
—. 2021d. XML Schema Tutorial. [Online] 2021d. [Citat: den 21 6 2021.] https://www.w3schools.com/xml/schema_intro.asp.
—. 2021e. XML Soap. [Online] 2021e. [Citat: den 30 6 2021.] https://www.w3schools.com/xml/xml_soap.asp.
—. 2021f. XML Tutorial. [Online] 2021f. [Citat: den 21 6 2021.] https://www.w3schools.com/xml/.

Bilagor

Bilaga 1 Exempel på riskbedömning av applikationsprogrammeringsgränssnitt med användning av riskanalys

I enlighet med informationshanteringslagen[100] ska relevanta risker som är förenade med applikationsprogrammeringsgränssnitt och de uppgifter som de behandlar också identifieras och informationssäkerhetsåtgärderna ska dimensioneras utifrån riskbedömningen. I syfte att effektivisera och förenhetliga riskhanteringen inom den offentliga förvaltningen har ledningsgruppen för den digitala säkerheten inom den offentliga förvaltningen VAHTI utarbetat en riskhanteringsanvisning[101] som kan också användas vid riskhantering som gäller applikationsprogrammeringsgränssnitt[102]. Själva anvisningen beskriver den allmänna riskhanteringsprocessen och i bilaga 4 till anvisningen[103] beskrivs standarder och bästa praxis inom riskhantering.

Europeiska kommissionen har i sin egen undersökning av införandet av applikationsprogrammeringsgränssnitt inom den offentliga förvaltningen identifierat ett antal risker som förenas med applikationsprogrammeringsgränssnitt tillsammans med metoder för att hantera dem[104]. Enligt undersökningen medför applikationsprogrammeringsgränssnitt tekniska, organisatoriska, juridiska och ekonomiska risker som ska identifieras och hanteras som en del av organisationens övriga riskhantering.

Som exempel i detta sammanhang används den informationsriskanalys som beskrivs i bilaga 4 till VAHTI-anvisningen. Analysen kan användas för att med hjälp av grundbegreppen inom informationssäkerhet utvärdera ett applikationsprogrammeringsgränssnitt eller en servicehelhet som består av applikationsprogrammeringsgränssnitt.

---

[100] Lagen om informationshantering, 4 kap., 13 §, (Tiedonhallintalaki 906/2019, 2019)
[101] VAHTI 22/2017 Riskhanteringsanvisning (på finska, svensk resumé), (Valtiovarainministeriö, VAHTI, 22/2017)
[102] Rekommendation om tekniska gränssnitt och elektroniska förbindelser (på finska, svensk resumé), sid 16, (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:21)
Katakri 2020 – tietoturvallisuuden auditointityökalu viranomaisille, T-03 (på finska), sid. 11, (Kansallinen turvallisuusviranomainen, Ulkoministeriö, 2020)
[103] VAHTI 22/2017 Riskhanteringsanvisning – Bilaga 4, (Valtiovarainministeriö, VAHTI, 22/2017)
[104] European Commision Joint Research Centre, Application Programming Interfaces in Governments: Why, what and how, sid. 53–55 (Vaccari, et al., 2020)

Genom detta är det möjligt att kartlägga de mest sannolika riskerna och hoten samt beskriva deras värsta konsekvenser.

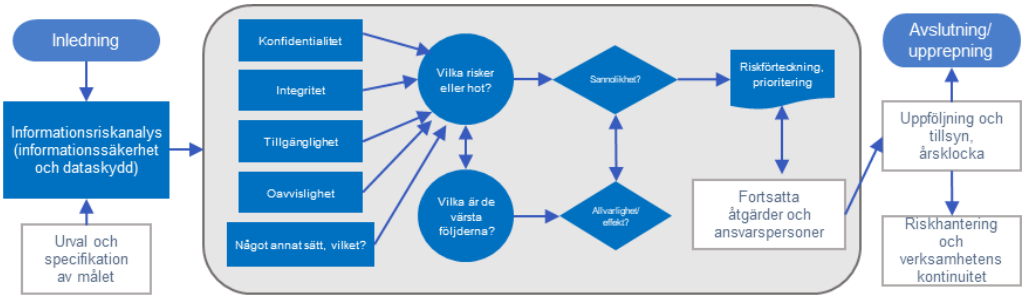

Bild 12 - Informationsriskanalys enligt bilaga 4 till anvisningen VAHTI 22/2017

Informationsriskanalys börjar genom att man väljer ett applikationsprogrammerings-gränssnitt eller en servicehelhet som består av applikationsprogrammeringsgränssnitt till objekt för riskhantering och identifierar de uppgifter som applikationsprogramme-ringsgränssnittet eller servicehelheten behandlar samt uppgifternas klassificering och ägare.

Informationsriskanalysen kan genomföras genom att bedöma risker och hot som gäl-ler konfidentialiteten, integriteten, tillgängligheten och obestridligheten av den inform-ation som applikationsprogrammeringsgränssnittet behandlar. Andra aspekter inom riskbedömning är till exempel hur kritiskt applikationsprogrammeringsgränssnittet är för organisationens verksamhet, beredskapskraven i fråga om kontinuitet och åter-hämtning samt interna och externa beroenden.

Efter att aspekterna valts ut bedöms vilka risker och hot som gäller applikationspro-grammeringsgränssnitt kan identifieras, och vilka de värsta konsekvenserna är om en risk eller ett hot blir verklighet. För de risker som identifierats på detta sätt uppskattas deras sannolikhet och allvarlighet. Utifrån detta erhålls en prioriterad riskförteckning (i allmänhet är prioriteten = sannolikhet x allvarlighet).

Till slut definieras riskhanteringsåtgärderna för varje risk, de personer som ansvarar för åtgärderna samt förfarandena och datumen för uppföljningen av risken. Riskhante-ringsåtgärder kan vara administrativa (till exempel åtgärder som gäller processen för utveckling av applikationsprogrammeringsgränssnittet, såsom specifikationer av test-nings- och besiktningsförfaranden) och tekniska (till exempel genomförandet av appli-kationsprogrammeringsgränssnittets testningsautomation och tekniska informations-säkerhetskontroller).