MINISTRY OF FINANCE

Public Administration API Principles

Public Sector ICT

Publications of the Ministry of Finance – 2022:14

Publications of the Ministry of Finance 2022:14

Public Administration API Principles

Ministry of Finance Helsinki 2022

Publication distribution

Institutional Repository for the Government of Finland Valto

julkaisut.valtioneuvosto.fi

Publication sale

Online bookstore of the Finnish Government

vnjulkaisumyynti.fi

Ministry of Finance

ISBN pdf: 978-952-367-915-3
ISSN pdf: 1797-9714

Layout: Government Administration Department, Publications

Helsinki 2022 Finland

Description sheet

28 February 2022

Public Administration API Principles

Publications of the Ministry of Finance 2022:14		**Subject**	Public Sector ICT
Publisher	Ministry of Finance		
Author(s)	Miina Arajärvi, Maaret Saukonoja and Pasi Vänttinen		
Language	English	**Pages**	64

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	978-952-367-915-3	**ISSN PDF**	1797-9714
Project number	VN/5386/2020		
URN address	https://urn.fi/URN:ISBN:978-952-367-915-3		

Kuvailulehti

28.2.2022

Julkisen hallinnon API-periaatteet

Valtiovarainministeriön julkaisuja 2022:14		**Teema**	Julkisen hallinnon ICT
Julkaisija	Valtiovarainministeriö		
Tekijä/t	Miina Arajärvi, Maaret Saukonoja ja Pasi Vänttinen		
Kieli	englanti	**Sivumäärä**	64

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	978-952-367-915-3	**ISSN PDF**	1797-9714
Hankenumero	VN/5386/2020		
Julkaisun osoite	https://urn.fi/URN:ISBN:978-952-367-915-3		

Presentationsblad

28.2.2022

API-principer för den offentliga förvaltningen

Finansministeriets publikationer 2022:14		**Tema**	Offentliga förvaltningens ICT
Utgivare	Finansministeriet		
Författare	Miina Arajärvi, Maaret Saukonoja och Pasi Vänttinen		
Språk	engelska	**Sidantal**	64

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	978-952-367-915-3	**ISSN PDF**	1797-9714
Projektnummer	VN/5386/2020		
URN-adress	https://urn.fi/URN:ISBN:978-952-367-915-3		

Contents

1 Introduction

According to the Programme of Prime Minister Sanna Marin's Government[1], the Government adds depth to the management of information policy, and the openness of public information will become the overarching principle of information policy. Among other things, this requires public actors to open public APIs unless there is a special reason for keeping them closed. The Ministry of Finance's project on opening up and using public data implements the objectives related to information policy and the opening and use of public data in the Programme of Prime Minister Marin's Government[2]. The project has been instituted for the period 30 April 2020–31 December 2022. The goals of the project include promoting the use of information and functionalities consistently through application programming interfaces (API).

This document presents the principles and support materials for the development of application programming interfaces (API) in public administration. The principles consist of recommendations and best practices for API development and the promotion of digitalisation in public administration. The support materials and examples provide practical instructions to support the adoption of the principles.

The principles support the implementation of the requirements provided for electronic data disclosure[3] in the Act on Information Management in Public Administration. The principles have been drawn up according to the European Commission's API Framework[4] taking into account, for example, the European Interoperability Framework with regard to technical and semantic interoperability[5]. Sector-specific regulations, such as the INSPIRE

1 Programme of Prime Minister Sanna Marin's Government (Valtioneuvosto, 2019:31)

2 Opening up and using public data project (Valtiovarainministeriö, 2021a)

3 Act on Information Management in Public Administration, sections 22 and 24 (Tiedonhallintalaki 906/2019, 2019)

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

5 European Interoperability Framework – Implementation Strategy (Euroopan Komissio, 2017)

Directive[6], the recommendations issued by the Information Management Board[7] and the national strategic goals for opening up and using public data[8].

The API principles and their support materials address API development more comprehensively than, for example, the Information Management Board's current recommendations, which apply to the technical APIs falling within the scope of the Act on Information Management in Public Administration[9]. The API principles cover the provision and use of information and functionalities through both internal and external APIs, regardless of the data transfer protocol used.

Authorities are free to develop the principles further for their own needs, for example with regard to their binding nature.

1.1 Goals

The purpose of the principles is to promote the provision and use of public-sector information and functionalities, primarily through APIs. The goal of the principles is to increase customer orientation, cooperation, semantic and technical interoperability, reusability, attention to information security and data protection, and quality in API development.

Customer orientation means taking the needs of potential API users into account throughout the life span of the API, from needs assessment to decommissioning. APIs developed in a customer-oriented manner meet the needs of their users and are constantly improved to better serve the user. Customer orientation increases user satisfaction and the utilisation rate of the API.

Customer orientation requires **cooperation** between the providers and users of information, functionalities and APIs. This cooperation can be internal or external. Internal cooperation encompasses cooperation between different levels, teams and units of the same organisation. External cooperation can involve cooperation between public

6 INSPIRE Directive (Euroopan parlamentin ja neuvoston direktiivi 2007/2/EY, 2019) and its national implementation (Laki paikkatietoinfrastruktuurista 421/2009, 2009)

7 Recommendations of the Information Management Board (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020-2021)

8 A government resolution on the opening up and use of public data is due to be published in spring 2022.

9 Information Management Board's Recommendation concerning technical interfaces and viewing access (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:21)

actors, between public actors and private sector operators, or cooperation with citizens. Cooperation not only promotes customer-oriented development, but also enables the sharing of competence, experiences and solutions between the parties.

Reusability means that the APIs and the information and functionalities offered by them are readily available and can be used when new solutions are implemented. This reduces overlapping work and solutions, speeds up development and improves productivity, as new solutions can be developed on top of existing information, functionalities and APIs.

Technical interoperability means the alignment of data transfer technologies[10]. **Semantic interoperability** means that the precise format and meaning of exchanged data and information is preserved and understood throughout exchanges between parties, in other words 'what is sent is what is understood'[11]. Technically and semantically interoperable APIs improve the transferability of information, speed up development and improve productivity.

Information security means taking into account the integrity, confidentiality and availability of the data being processed throughout the life span of the API. **Data protection** means protecting personal data processed through the APIs according to requirements.

Quality means that the features or capabilities of the APIs meet the needs and expectations of their users[12]. High-quality APIs increase user satisfaction and the utilisation rate of the APIs. Quality also speeds up development and thus increases productivity.

1.2 Target group

The target group of the principles consists of:

- public organisations such as government agencies and public bodies, municipalities and joint municipal authorities, wellbeing services counties, and higher education institutions and other education institutions;
- companies, corporations or other operators that process public-sector information or perform public administrative tasks; and
- companies, corporations or other operators that provide data-processing or information-management services or solutions to public-sector organisations.

10 Definition of technical interoperability (Valtiovarainministeriö, 2021b)
11 Definition of semantic interoperability (Valtiovarainministeriö, 2021b)
12 The definition of quality is based on the OECD's ISO definition (OECD, 2002)

1.3 Limitations

The principles do not apply to user interfaces intended for end users.

The principles are not an exhaustive manual or design guide to APIs. The principles do not designate technologies, data transfer formats or data models for use, but give examples of these to guide the reader.

Neither do the principles contain sector-specific instructions or specifications, which can be developed on top of the principles in a sector-specific manner.

2 What are APIs?

2.1 Definition

Application Programming Interfaces or APIs are documented interfaces that facilitate the exchange of data or functionalities between software, applications or systems[13]. 'API', 'application programming interface' and technical interface[14], as defined in the Act on Information Management in Public Administration, are identical in meaning for the purposes of this document.

Thus defined, 'API' covers both web-based REST, SOAP or GraphQL APIs and interfaces built on file- or database-based protocols or other protocols. It is essential that the **API provides the information or functionality in a machine-readable, documented format so that another program, application or system can use it programmatically.**

It should be noted that APIs are not user interfaces intended for end users. Rather, the user of an API is always another program, application, application component or system.

2.2 Value chain

APIs can be viewed as independent products connected to a value chain[15] (Figure 1).

The value chain begins with the provider of a **digital commodity** in possession of a product, the digital commodity, that is valuable to other parties. A digital commodity can consist of information, such as statistics or register data, or functionalities such as tax rate calculation, frame-of-reference conversion or data reporting functionalities.

The API provider provides the API through which other parties can use the digital commodity provider's product. The API provider can be the same or a different party than the digital commodity provider.

13 This definition is adapted from that in the EU publication, pp. 18–19 (Vaccari, et al., 2020)

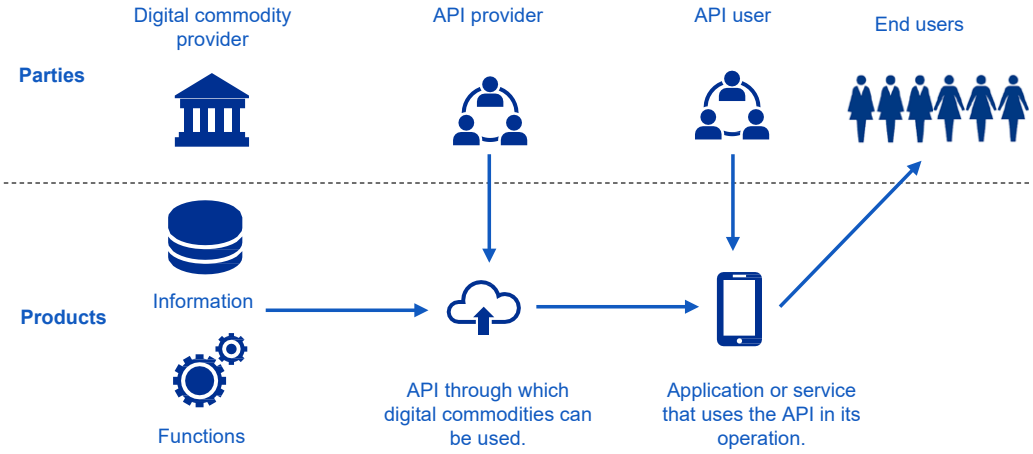
14 Act on Information Management in Public Administration, section 2, paragraph 11 (Tiedonhallintalaki 906/2019, 2019)

15 This value chain is adapted from the value chain presented on p. 20 of the EU publication. (Vaccari, et al., 2020)

The API user uses the API and the information or functionality provided by it in the user's own application or service. The API user can be the same or a different party than the API provider.

An application or service can also have **end users**. End users do not directly use APIs, but rather the application or service that uses the API in its operation.

Figure 1. The API value chain[16]



16 This value chain is adapted from the value chain presented on p. 20 of the European Commission's publication (Vaccari, et al., 2020).

EXAMPLE

- The Finnish Tax Administration possesses information on personal tax numbers and their validity[17]. The Tax Administration is a digital commodity provider.
- The Tax Administration has developed an API that provides a functionality[18] which others can use to programmatically verify the validity of a tax number. The Tax Administration is an API provider.
- A private sector operator develops an information system for managing construction site passes. When a new pass is created, the information system uses the Tax Administration's API to verify the validity of the individual's tax number. In this case, the private sector operator is an API user.
- Employees in the construction sector, such as site managers, use the information system for pass management. They are end users.
- The Tax Administration also offers a web interface, through which tax numbers can be verified manually, for example with a web browser or mobile device[19]. In this case, the Tax Administration is offering an application or service directly to the end users. If the Tax Administration uses its own API in the tax number verification functionality via web interface, the Tax Administration is also a user of its own API.

17 Finnish Tax Administration's tax number register (Verohallinto, 2021d)

18 The Finnish Tax Administration's Vero API (Verohallinto, 2021b)

19 Web interface provided by the Finnish Tax Administration (Verohallinto, 2021c)

2.3 Typology

APIs can be internal or external in type. Table 1 presents the different types of APIs and their common features.

Table 1. API types

API type		Use limitation	Potential user	Classification of the processed data
INTERNAL	Internal API	Yes	Own organisation	Classified information Confidential information, including personal data Public information
EXTERNAL	Partner API	Yes	Own organisation Other governmental actors Other private sector operators Others	Classified information Confidential information, including personal data Public information
	Public API	No	Anyone.	Public information

Internal APIs are intended solely for the organisation's own use. External APIs may be restricted to certain parties (**partner API**) or open, unrestricted interfaces (**public API**).

Internal or external APIs intended for specific partners can be used to process public information, confidential information, personal data or classified information. Public APIs only process public information.

The users of internal APIs and APIs intended for specific partners are normally identified (authenticated) and the user's access rights are verified (authorised). Access right verification (authorisation) is not required in public APIs, because they only offer public information. In some cases, the users of public APIs can also be authenticated, such as for collecting data on API users for monitoring or communications purposes.

EXAMPLE

- Organisations such as municipalities, government agencies or education institutions can have their own registers, such as a client or student register. The organisation develops an API for retrieving information from the register, and the organisation's other information systems or applications can use the API to search for information in the register according to certain criteria. If the API is intended solely for the organisation's own use, **it is an internal API**.
- National Land Survey of Finland provides a query service[20] for requesting identifying data, characteristic data and owner data on buildings. Using the service requires the Digital and Population Data Services Agency's authorisation and its use is thus restricted to specific parties. **This is a partner API**.
- The Finnish Transport Infrastructure Agency provides open APIs[21] that can be used to download and view geographical datasets related to the road, rail and waterway network. **This is a public API, the use of which does not require registration or authentication.**

2.4 Life span

APIs have life spans that begin from needs assessment and end with decommissioning. The life span covers all phases between these end points, namely specification and design, competitive tendering and procurement, implementation and development, deployment, maintenance and decommissioning[22]. The life span of an API is iterative, meaning that these phases are repeated until all versions of the API have been decommissioned.

It should be noted that the life span of an API may be different from that of the information or functionality provided by it. The life span of an API can also begin later than that of the information or functionality provided by it. It is possible that the life span of the information or functionality remains unchanged, while the features or functionalities of the API are developed, new versions of the API are created and old versions are decommissioned. The life span of an API can also end before that of the information or functionality provided by it, for example because it is no longer necessary or its technology has become obsolete.

20 National Land Survey of Finland query service (Maanmittauslaitos, 2021b)

21 Finnish Transport Infrastructure Agency open APIs (Väylävirasto, 2021)

22 Adapted from the information system life span, p. 26 (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:65)

3 Principles

API principles have been divided into three levels: strategic, tactical and operative.

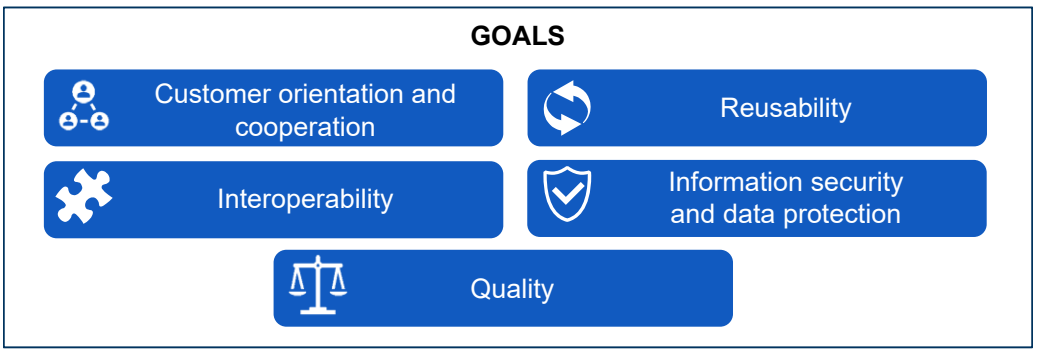
Strategic principles apply to the organisation's management. These principles describe how the direction and goals of API development should be defined and how APIs should be taken into account in the development of operations.

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.

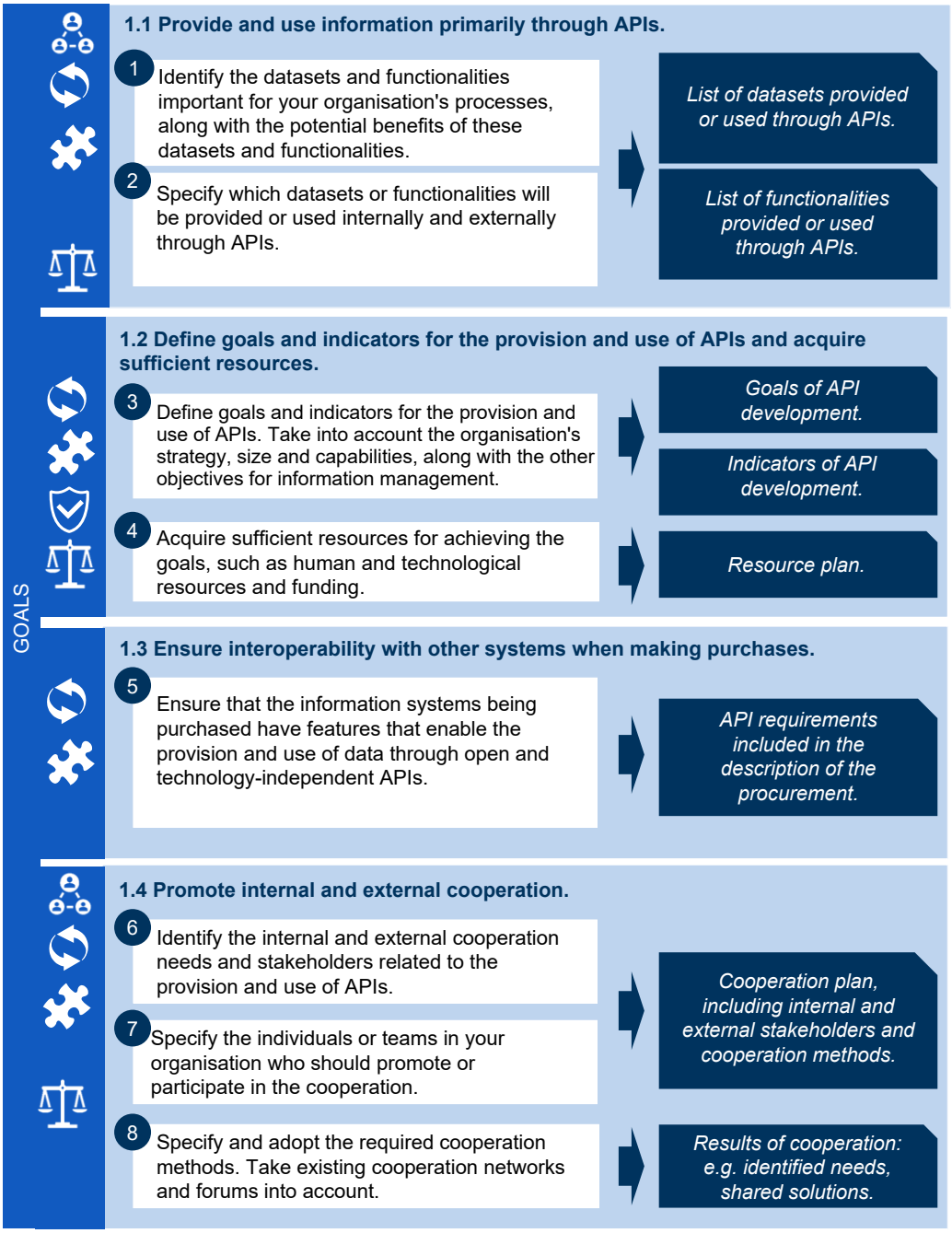
The principles are described in sections 3.1, 3.2 and 3.3. They support the achievement of the goals set for APIs (Figure 2). Principle-specific goals are indicated by the symbols below.

Figure 2. Goals



3.1 Strategic level

Figure 3. Strategic principles



Principle 1.1 Provide and use information primarily through APIs

Identify the datasets and functionalities important for your organisation's processes and core tasks that can be provided or used through APIs. Also determine their potential benefits. Please note that such datasets and functionalities can be owned by your organisation or others. The potential benefits of datasets and functionalities can be related to the development or needs of your own organisation or its stakeholders.

The following questions can be used to define datasets or functionalities provided or used through APIs.

- What information or functionalities are available to your organisation?
- What or what kind of information does it need more of?
- What kind of information would support management by knowledge-based management?
- What are your stakeholders' information or functionality requirements?
- What information is needed regularly, in machine-readable format or as up-to-date as possible?
- What functionalities would be necessary or possible to provide or use digitally?
- Also consider what kinds of benefits, risks and costs the provision and use of information and functionalities will entail for your organisation.

Specify which or what kinds of datasets or functionalities can be provided or used internally and externally through APIs. Identify the administrators of the information or functionalities. Internal provision and use can be implemented through internal APIs. External provision and use can be implemented through partner APIs or public APIs, depending on the classification of the information. Public APIs can create new operating methods, outputs and partnerships, and thus have a significant impact on the organisation's operations.

Take into consideration the requirements of legislation on the right of access to information, the disclosure of information and the provision of data in machine-readable format[23]. It is also important to identify confidential information. Also take into

23 For example, section 22 of the Act on Information Management in Public Administration (Tiedonhallintalaki 906/2019, 2019) and the Information Management Board's Recommendation concerning technical interfaces and viewing access (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:21).

account any modification required to the information, such as pseudonymisation or anonymisation[24].

OUTPUTS

- List of datasets potentially provided or used through APIs.
- List of functionalities potentially provided or used through APIs.

BENEFITS

- These lists make it easier for the organisation to identify datasets and functionalities with potential benefits, focus its API development on them and thereby promote needs-oriented API development.
- Focused and needs-oriented development improves the customer-orientation, cooperation, reusability, interoperability and quality of APIs

SUPPORT MATERIALS

Examples of APIs that provide information or functionalities:

- The City of Helsinki has opened an Issue Reporting API[25] for giving feedback to the City, such as reporting broken traffic signs or potholes. The API can also be used to search for feedback published in the system. This API provides both functionalities, feedback and information.
- Finna offers an open API[26] for making searches in the materials of Finnish libraries, archives and museums. This is an information-providing API.

24 Pseudonymised and anonymised data website (Tietosuojavaltuutetun toimisto, 2021), also see Kyberturvallisuuskeskuksen Tunnisteet ja tietosuoja, anonymisointi ja sen rajat -opas (Traficom, 2021) (Traficom, Kyberturvallisuuskeskus 2021)

25 The City of Helsinki's Issue Reporting API (Helsingin kaupunginkanslia, 2020), also see the definition of 'feedback API' by the 6Aika project (6Aika-kaupungit, 2016)

26 Finna's open API (Kansalliskirjasto, Finna, 2021)

The following materials can also be helpful in identifying information or functionalities to be provided through APIs and assessing their potential benefits:

- The Recommendation for an information management model[27] published by the Information Management Board.
- An assessment method for identifying and sharing information with potential benefits (benefits, risks and costs)[28].
- An information management map for identifying the current state of statutory information disclosures from shared government information resources[29].

Principle 1.2 Define goals and indicators for the provision and use of APIs and acquire sufficient resources

Define goals for the provision and use of APIs. The goals should serve the organisation's strategy and processes and be in line with the goals of other information management. The goals should be realistic with respect to the organisation's size and capabilities. They can be described together with other information management goals or a data strategy, or in a separate API or integration strategy.

Define the necessary indicators for the provision and use of APIs. They can be process, performance or impact indicators [30] (see Figure 4). Process indicators are used to guide operations or ensure their quality, such as the achievement of service levels. Performance indicators are normally used to measure the direction and magnitude of a change, such as the achievement of the goals set for APIs. Impact indicators describe the results of operations in relation to a social goal, problem or need, such as the impact of APIs on the development of government services or knowledge-based management. Choose indicators that serve your organisation's monitoring needs and can be tracked. Indicators can be tracked at the strategic, tactical and operative levels of the organisation.

27 Recommendation for an information management model (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:29)

28 The assessment method will be published in March 2022 in the avoindata.fi service maintained by the Digital and Population Data Services Agency.

29 Information management map of public administration in the tutkihallintoa.fi service (Valtiovarainministeriö, 2022)

30 Choice of indicators (Hyvän Mitta, 2021)

Acquire the resources required for achieving the goals. Take into account the provision, use and maintenance of APIs when determining the required resources. The resources can consist of human resources, expertise or technological resources. The acquisition and maintenance of resources and competence requires funding. To help identify and meet your competence, resource and funding needs, discuss them with the teams or individuals responsible for information management in your organisation. Develop the competences of your organisation's own personnel if possible. Make use of teams or individuals already working with information management, enterprise architecture, application development or integrations.

Figure 4 presents an example of the goals, indicators and required resources of API development. In the example figure, the goals of API development have been derived from an imaginary organisation's strategic goals.

Figure 4. Example of goals, indicators and resources

OUTPUTS

- API development goals. Can be included in, for example the information management goals, data strategy or integration strategy.
- API development indicators that serve the organisation's monitoring needs and can be tracked.
- A resource plan for achieving the goals, taking into account human and technological resources and funding.

BENEFITS

- By setting goals and drawing up a resource plan, the organisation can prioritise API development, divide it into stages, and allocate resources to development, resulting in orderly and systematic development that serves the organisation's other goals.
- The organisation can use various indicators to track changes in API development and the achievement of goals.
- Orderly and systematic development and monitoring improves the reusability, interoperability, attention to information security and data protection, and quality of APIs.

SUPPORT MATERIALS

Examples of goals related to the provision and use of APIs and of putting them into perspective with the organisation's other strategies:

- The City of Helsinki Data Strategy[31] addresses the provision and use of information through APIs.
- API development in the Finnish Tax Administration[32] presents the use of APIs in the Tax Administration's strategy (in Finnish).
- APIs as part of the strategic goals of the government resolution on the opening up and use of public data[33].

31 City of Helsinki Data Strategy, Chapter 5 (Digitaalinen Helsinki, 2021)

32 API development in the Finnish Tax Administration (Verohallinto, 2019)

33 A government resolution on the opening up and use of public data is due to be published in spring 2022.

Also see the following materials for help in identifying goals and indicators:

- The Hyvän Mitta (Measuring Good) project[34] provides more information on impact, the impact chain, and choice of indicators (in Finnish).
- Thesis for the Metropolia University of Applied Sciences: Measuring Strategic Aims[35] includes, for example a "hallmarks of a good indicator" checklist and a sample set of indicators for ICT software.

Principle 1.3 Ensure interoperability with other systems when making purchases

Ensure that the information systems being purchased have features that enable the provision and use of data through open and technology-independent APIs. Examples of required features:

- Pre-made APIs in off-the-shelf software, which can be used to provide the information or functionalities contained in the system to other systems. APIs should be based on open, technology-independent and widely used protocols and standards.
- Tools for developing completely new APIs or modifying existing APIs to better serve their purpose.
- Tools for integrating the system with APIs provided by other systems.
- A licensing model or terms that enable the provision, use and reuse of the information and functionalities in the system both within the organisation (internal API) and externally though external APIs (partner API, public API).
- Management of access rights and use to ensure compliance with the requirements concerning confidential information, classified information and personal data.

In information system procurement, **the requirements related to the provision and use of information and functionalities must be included in the specification of the object of procurement in the call for tenders**[36]. It is important that the organisation's information management are involved in the procurement of new information systems from the beginning.

34 Hyvän Mitta (Hyvän Mitta, 2021)

35 Measuring Strategic Aims (Rautio, 2015)

36 Act on Public Procurement and Concession Contracts (Laki julkisista hankinnoista ja käyttöoikeussopimuksista 1397/2016, 2016).

OUTPUTS

- API requirements included in the procurement description.

BENEFITS

- When the requirements related to the provision and use of information and functionalities are taken into account immediately at the information system procurement stage, the information system can be aligned to the organisation's current ICT environment and adapted to future changes in it.
- The use of open, technology-independent and widely used protocols and standards combined with a flexible licensing model also reduces the risk of vendor lock-in.
- Information systems capable of providing and using open, technology-independent and widely used APIs improve system reusability and technical interoperability.

SUPPORT MATERIALS

Sources of support and additional information for procurement processes:

- The online service of the Public Procurement Advisory Unit[37].
- The framework agreement materials[38] maintained by HANSEL.
- The Information Management Board's collection of recommendations on the application of certain information security regulations[39], containing recommendations on taking the life span of information into account in information systems, including in the competitive tendering and procurement stages (in Finnish).

37 Public Procurement Advisory Unit (Julkisten hankintojen neuvontayksikkö, 2021)

38 Framework agreements (Hansel, 2021)

39 Information Management Board's collection of recommendations on the application of certain information security regulations (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:65)

Principle 1.4 Promote internal and external cooperation

Identify the internal and external cooperation needs related to the provision and use of APIs. Cooperation needs can involve, for example:

- identifying or sharing ideas or needs;
- developing or sharing goals, operating models, instructions or guidelines;
- developing or sharing solutions; and
- sharing competence or experiences.

Identify the stakeholders with whom there is a need to cooperate. Please note that cooperation happens at different levels of the organisation. Possible stakeholders include:

- the management of your own or another organisation;
- the individuals or teams responsible for the development of information management in your own or another organisation; and
- the development and maintenance teams of your own or another organisation.

Specify the individuals or teams in the organisation who should promote or participate in the cooperation. Meet with them to think about what kind of cooperation structure could improve and enhance the use of information and functionalities both within and without the organisation through APIs. In a small organisation, this can mean just a few individuals. If this is the case, cooperation and sharing development experiences in networks is particularly important.

Specify and adopt the required cooperation methods. Take existing cooperation networks and forums into account.

OUTPUTS

- Cooperation plan, including internal and external stakeholders and cooperation methods.
- Cooperation outputs, such as identified needs, shared solutions or experiences, and the development of competence.

BENEFITS

- With networking, cooperation and continuous dialogue organisations can identify the changing needs of their internal and external stakeholders and develop APIs to meet those needs.
- In addition, cooperation enables the sharing of competence across organisational boundaries as lessons, experiences and solutions are shared between individuals and organisations.
- Identifying stakeholder needs improves the customer-orientation, cooperation, reusability, interoperability and quality of APIs.

SUPPORT MATERIALS

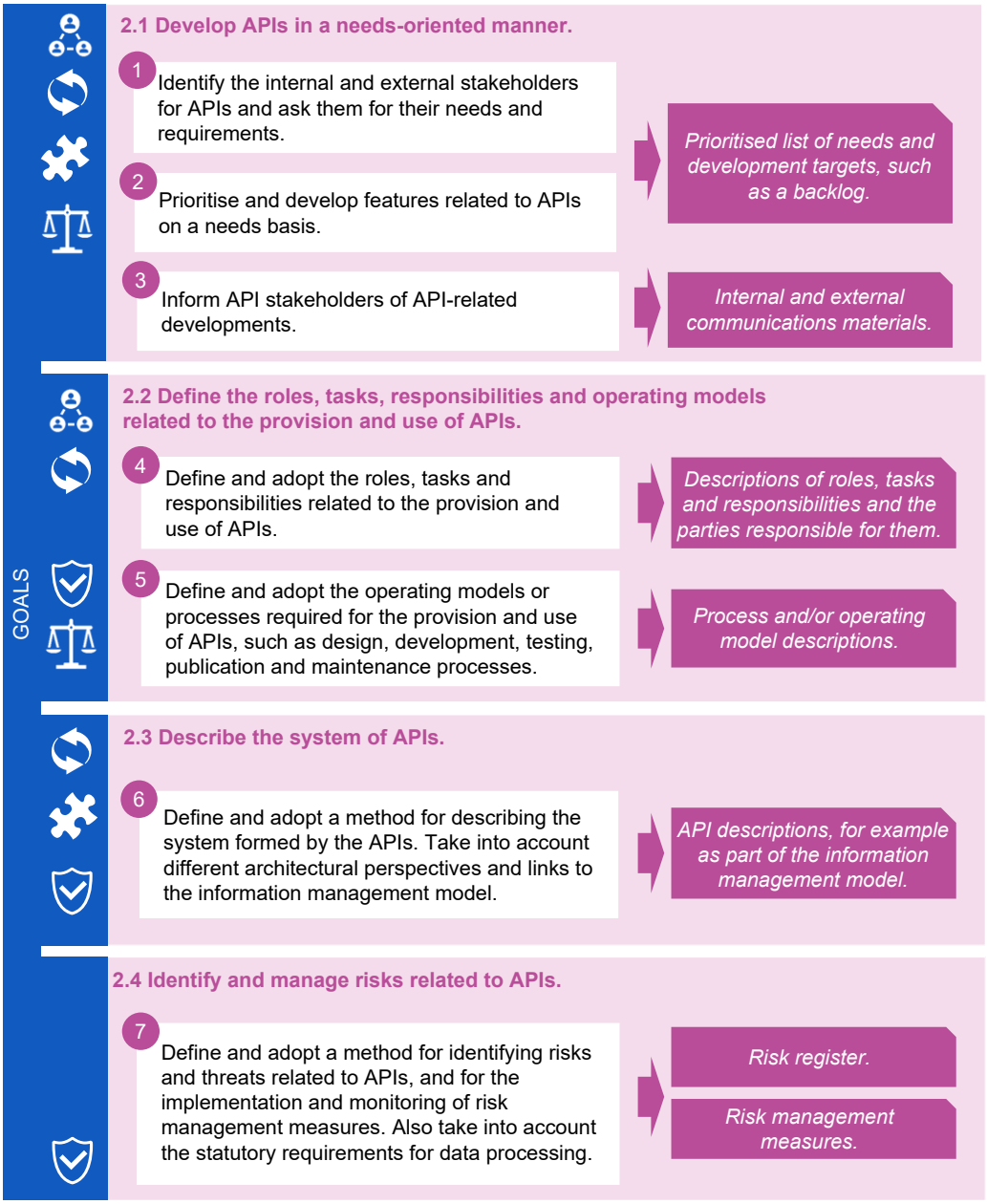
Examples of existing cooperation forums which the organisation's personnel can join:

- The Open Data Network (in Finnish)[40]
- National Land Survey of Finland's cooperation groups[41]
- eInvoice Forum[42]
- API-Suomi Facebook group (in Finnish)[43]
- Github communities[44]
- Finnish Standards Association's ICT standardisation groups (in Finnish)[45].

40 The Open Data Network (Varsinais-Suomen liitto, 2021)
41 National Land Survey of Finland's cooperation groups (Maanmittauslaitos, 2021c)
42 eInvoice Forum (TIEKE Tietoyhteiskunna Kehittämiskeskus Ry, 2021)
43 API-Suomi Facebook group (Honkanen, 2021)
44 GitHub communities (GitHub, 2021)
45 ICT standardisation groups (Suomen standardisoimisliitto SFS Ry, 2021b)

3.2 Tactical level

Figure 5. Tactical principles



Principle 2.1 Develop APIs in a needs-oriented manner

Identify the internal and external stakeholders for APIs and ask them for their needs and requirements. Possible stakeholders include:

- Parties in the value chain, such as the digital commodity provider, API provider, and API user or potential user.
- Your own or another organisation's employees, teams or groups, management, designers, developers, testers or administrators working with information management.

Needs can be related to API functionalities or non-functionalities, such as availability, usability, data integrity, service level, or the developer or end user experience. Also take into account the requirements arising from legislation[46] **and changes in legislation**. Information on needs can be collected through surveys, feedback channels, cooperation groups, workshops or other cooperation methods. Collecting information on the needs of users or potential users can be difficult in case of a public or open data API whose users cannot be identified. But even in such cases, you can still publish an open feedback channel for users.

Prioritise and develop features related to APIs on the basis of needs. Take needs into account for the entire life span of APIs, from the needs assessment to decommissioning: specify and plan, invite tenders and purchase, implement and develop, and maintain and retire features related to APIs according to needs and requirements.

Inform API stakeholders of API-related developments. Take both internal and external stakeholders into account in communications.

46 For example the requirement of electronic disclosure of information of a regularly repetitive character and standard content between information systems via technical interfaces, provided for in the Act on Information Management in Public Administration (Tiedonhallintalaki 906/2019, 2019), and the statutory requirements for the processing of classified documents (Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa, 1101/2019). Also see the Information Management Board's recommendations (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020-2021).

OUTPUTS

- Prioritised list of needs and development targets related to APIs, such as a backlog.
- Internal and external communications materials.

BENEFITS

- Identifying needs and collecting information on them helps to allocate API development resources and measures effectively, so that they fulfil the needs which provide the greatest benefits to the organisation and users of the API.
- Informing stakeholders of API development gives them the opportunity to react in time to future changes and plan their own operations with a view to planned development areas.
- Correctly allocated resources, useful APIs that meet user needs, and active communications improve the customer-orientation and cooperation, reusability, interoperability and quality of APIs.

SUPPORT MATERIALS

Examples of open channels published by government organisations that can be used to collect information on stakeholder needs or communicate with stakeholders:

- The Digitraffic website[47], with announcements related to APIs and information on the status of APIs. The site also contains links to open Google groups that contain information on, for example, API development and downtime.
- The Vero API website[48], which offers a look at planned APIs and contains an observations form with which API users can give feedback or development ideas to the Finnish Tax Administration.

47 Open data and APIs related to transport (Fintraffic, 2021)

48 Vero API (Verohallinto, 2021b)

Principle 2.2 Define the roles, tasks, responsibilities and operating models related to the provision and use of APIs

Define and adopt the roles, tasks and responsibilities related to the provision and use of APIs. Remember to consider tasks related to the overall management of APIs, such as information model maintenance, risk management and architecture guidance, along with tasks related to the provision and use of APIs and responsibilities for the management of information processed through the APIs. Utilise the organisation's existing structures and good practices where possible. In practice, the use of APIs means integration with an API. Both APIs and integrations have limited life spans, and their various phases should be taken into account in the tasks:

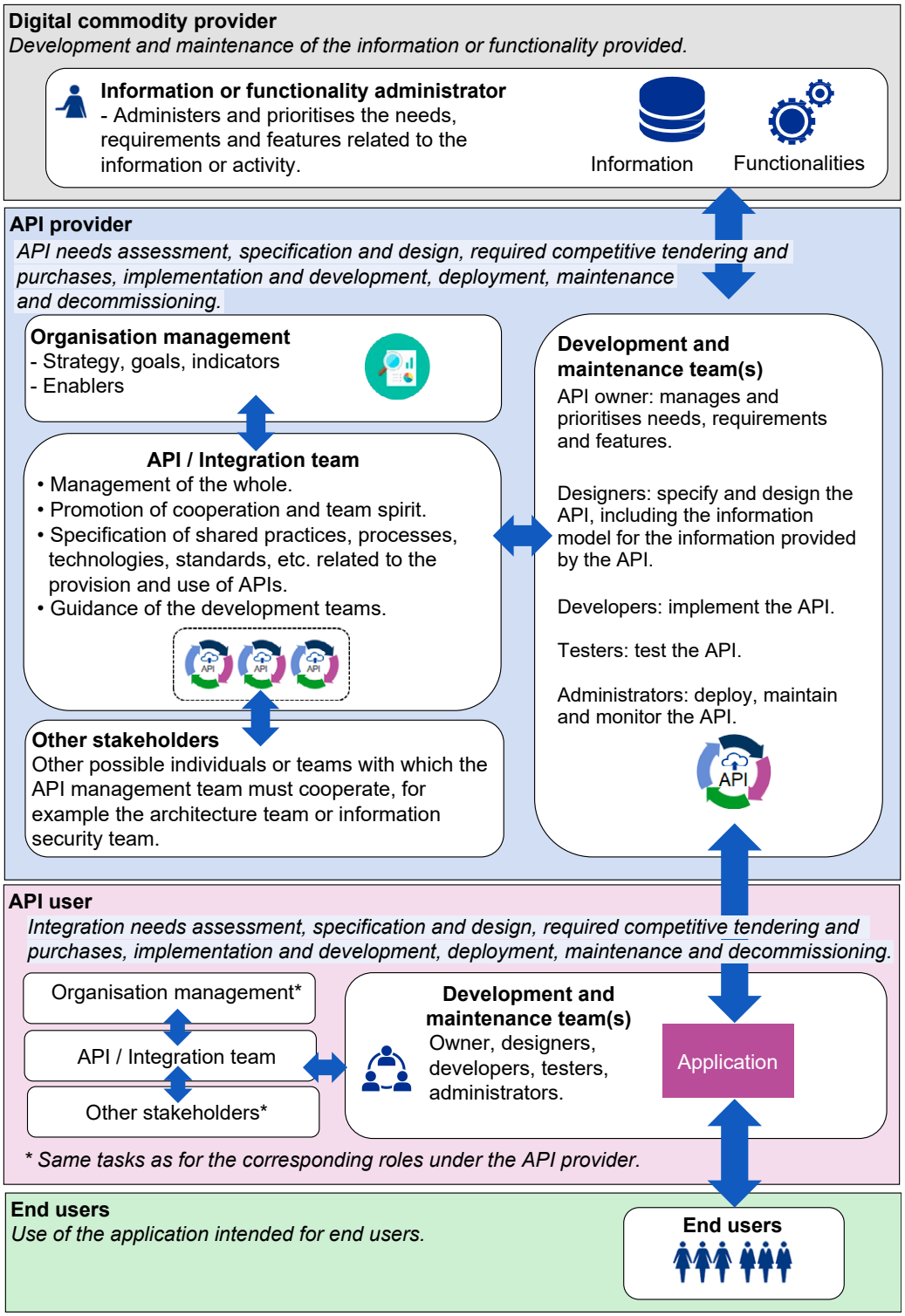
- needs assessment and prioritisation for the API or integration;
- specification and design of the API or integration, taking into account information security and data protection;
- competitive tendering and procurements related to the API or integration;
- implementation and development of the API or integration;
- deployment of the API or integration;
- maintenance and support of the API or integration; and
- decommissioning of the API or integration.

Some tasks related to the life span of the API, such as implementation and development or maintenance and support, can be outsourced to partners. Remember to specify the roles, tasks and responsibilities of your own organisation and those of your partners in the role, responsibility and task descriptions.

Define and adopt the operating models or processes required for the provision and use of APIs, such as design, development, testing, publication and maintenance processes. When describing operating models and processes, also take into account other public and private organisations closely connected to the operating model or process in addition to your own organisation.

Figure 6 presents one example of the various actors in the API value chain and their roles, tasks and responsibilities, taking into account both the overall management and the provision and use of APIs. The example seeks to clarify the roles, tasks and responsibilities. A large organisation can allocate these tasks to different individuals and teams. In small organisations, individual employees will be responsible for several of the tasks assigned to different teams or roles in the example figure. The size and existing structure of the organisation are key when thinking about operating models.

Figure 6. An example of actors and their roles and responsibilities



OUTPUTS

- Descriptions of roles, tasks and responsibilities and the parties responsible for them.
- Process and/or operating model descriptions.

BENEFITS

- Defining and describing the roles, tasks, responsibilities and operating models related to APIs help the organisation and API users understand the API value chain of the API(s).
- Taking the entire life span into account in specifications and descriptions is important to ensure that not only development tasks, but also the tasks related to the continuity and recovery of production are performed.
- Understanding the API value chain and considering the entire life span of the API improve the customer orientation and cooperation, reusability, information security and data protection, and quality of APIs.

SUPPORT MATERIALS

Examples of suitable operating models or methods for API and integration development:

- ApiOpsCycles provides a method and tools for the various stages of API development[49].
- DevOps (Development and Operation), based on the principles of agile development, continuous integration, continuous deliveries and automation[50].
- DevSecOps (Development, Security and Operation), which expands DevOps by integrating information security more closely in each stage[51].

49 ApiOpsCycles (APIOps Cycles TM, 2021)

50 Several sources, including (ite wiki, 2021) and (DevOps.com, 2021)

51 Several sources, including DevSecOps Fundamentals, p. 17 (Department of Defence, United States of America, 2021) and DevSecOps Manifesto (DevSecOps, 2021)

Principle 2.3 Describe the system of APIs

Define and adopt a method of describing the overall system of APIs. It is important to be able to manage what APIs are provided, to whom and why, along with what APIs are used, from whom and why. The APIs provided and used can be the organisation's own internal APIs or external APIs (partner API, public API). External API providers or users can be national actors, such as other public organisations or private organisations, or international actors, such as other EU Member States or international commercial organisations.

Principle 3.3 Secure, test, version, document and publish the APIs defines the required contents for the documentation of individual APIs. This principle specifies the metadata and reference information that must be described and managed as part of the information management model, enterprise architecture or other overall description.

Use the organisation's existing practices for describing enterprise and solution architectures when describing the system of APIs. Take into account the perspectives of different architectures and links to the information management model in the description[52]:

- From the perspective of operations architecture, APIs participate in the implementation of a process or functionality. They can be linked to the process through an information resource or information system, for example.
- From the perspective of information architecture, APIs process information from one or more information resources.
- From the perspective of IT system architecture, APIs are connected to an information system.
- From the perspective of technology architecture, APIs use one or more technology resources.
- From the perspective of integration architecture, APIs are connected to one or more interfaces between information systems, or information flows.
- From the perspective of information security architecture, APIs cause information risks that must be identified and managed through risk management measures.

52 Act on Information Management in Public Administration, section 5 (Tiedonhallintalaki 906/2019, 2019), also see Recommendation for an information management model (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:29)

- From the perspective of the information management model, API descriptions add detail to the descriptions of the information management model[53]. Descriptions for the information management map of public administration[54] and description of document publicity[55] can be derived from the information management model.

The aspects of APIs that must be described are:

- Title: Name, identifier or other identifying information by which the API can be distinguished from other APIs.
- Purpose: Brief verbal description of what the API is used for.
- Owner: The person or team responsible for the management, needs, requirements and features of the API. For example, if the API is part of an information system, the information system owner can also be the API owner. If the API is its own, separate product, it must have a clearly defined owner.
- Life span: Life span status, describing the current stage in the life span of the API. Life span statuses can be derived from the various phases of the API life span, namely specification and design, competitive tendering and procurement, implementation and development, deployment, maintenance and decommissioning. At their simplest, the statuses could be, for example: in development / in use / being phased out / decommissioned.
- Information flow: Links to the interfaces between information systems, or information flows, in which the API is used.
- Provider: The API provider and information system connected to the API, if any.
- Users: A list of the users of the API. If individual users are not known or identified, for example in the case of an open public API, a description of the intended users will suffice.
- Processed data: If the API processes data, describe the relationship to the data, dataset, information resource or data group. Also take into account any personal data and confidential data contained in the processed data.
- Technologies: a description of the technology resource used by the API.

53 Recommendation for an information management model (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:29), also see Recommendation concerning technical interfaces and viewing access (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:21).

54 Information management map of public administration in the tutkihallintoa.fi service (Valtiovarainministeriö, 2022)

55 Act on Information Management in Public Administration, section 28 (Tiedonhallintalaki 906/2019, 2019)

The descriptions must be kept up to date. Use automation in the formation and maintenance of data where possible.

Figures 7 and 8 include examples of an API description from the perspectives of the API provider and user as part of the organisation's information management model. The example has been drawn up according to the Information Management Board's Recommendation[56] for an information management model based on the Act on Information Management in Public Administration[57]. The figures are fictitious and illustrative, although they are based on the Incomes Register API[58] actually provided by the Finnish Tax Administration for automatic reporting of pay information to the Tax Administration.

56 Recommendation for an information management model (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:29)

57 Act on Information Management in Public Administration, section 5 (Tiedonhallintalaki 906/2019, 2019)

58 Incomes Register technical interface (Verohallinto, 2021a)

Figure 7. Recommendation for an API description from the API provider's perspective as part of the information management model.

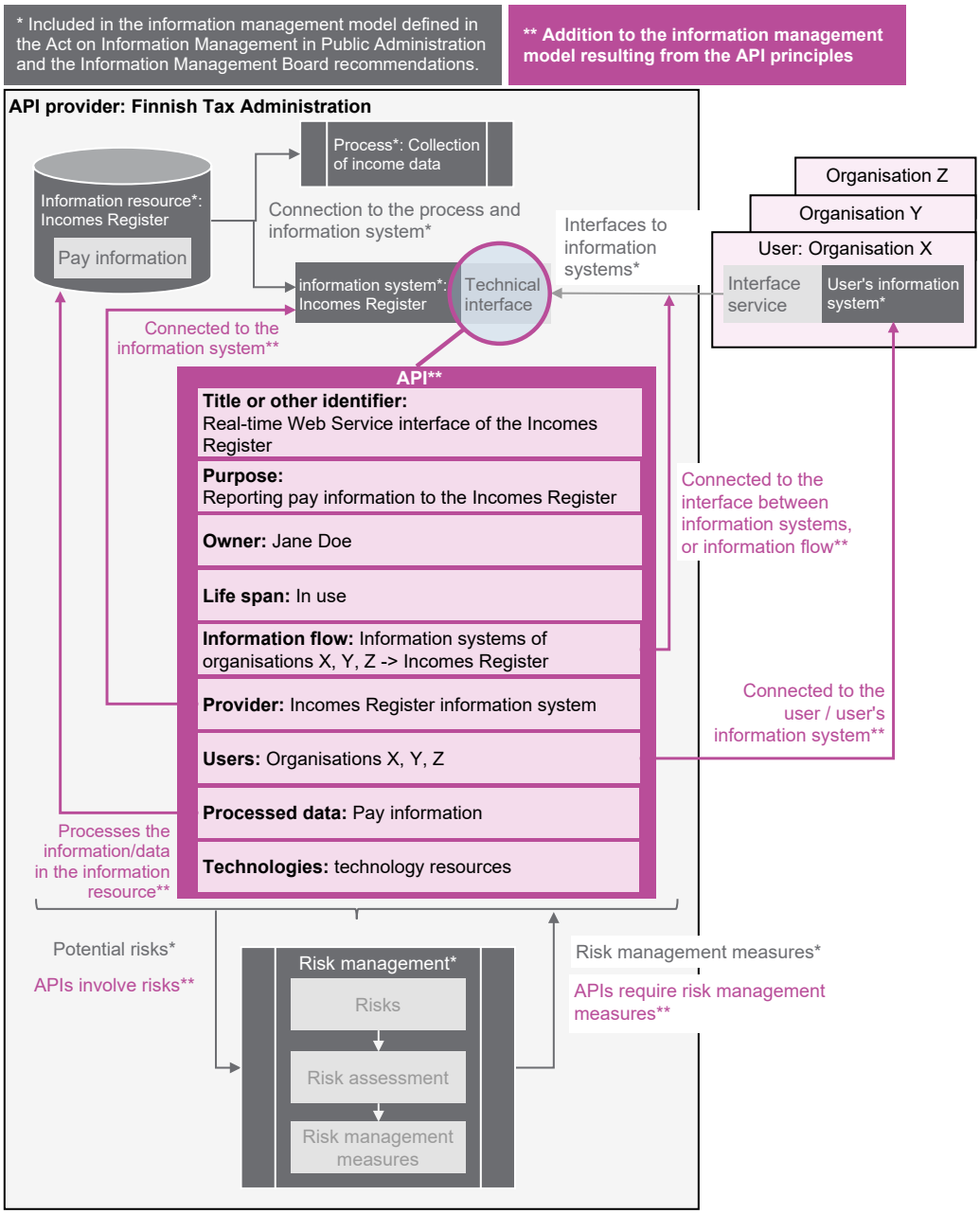
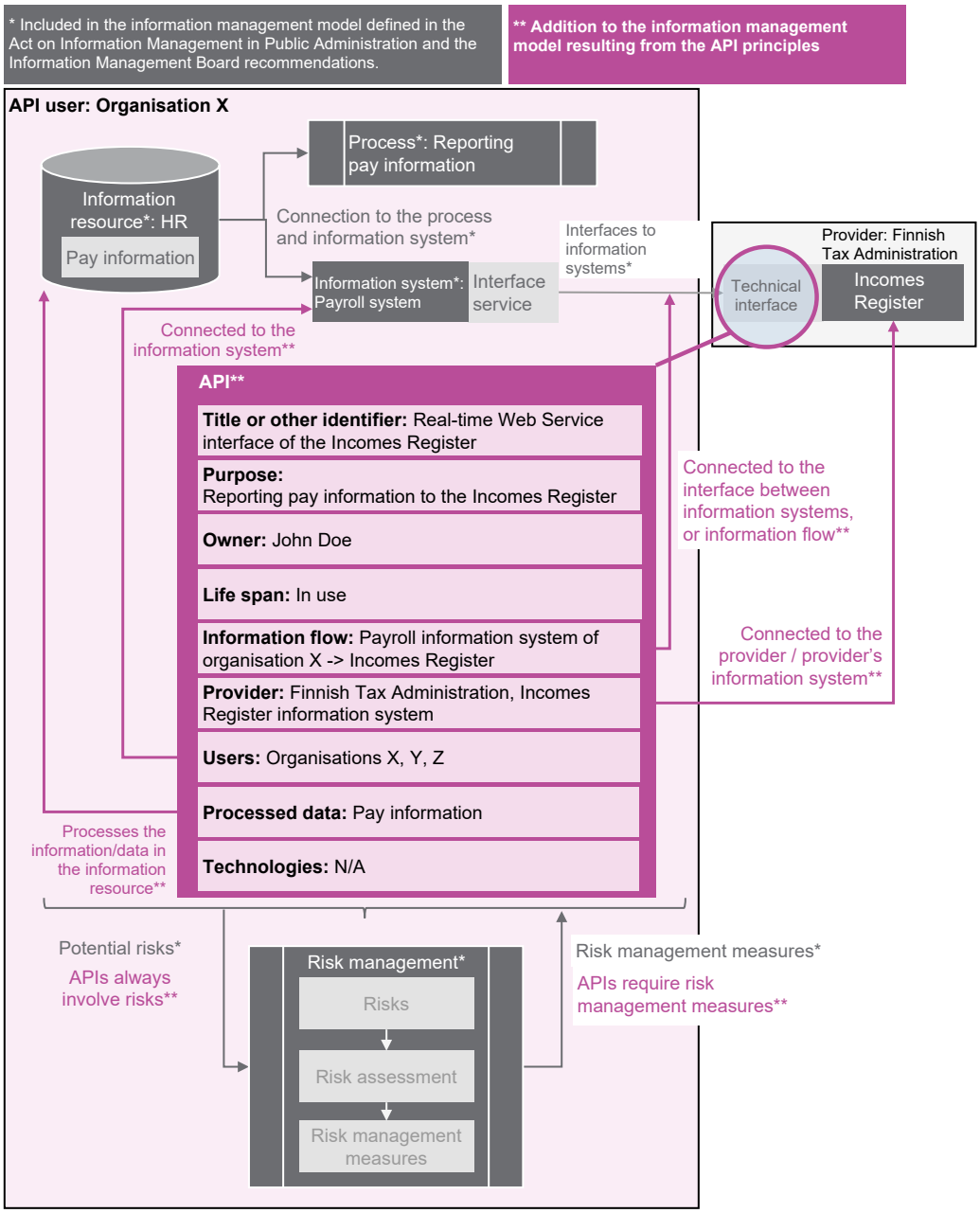


Figure 8. Recommendation for an API description from the API user's perspective as part of the information management model.



OUTPUTS

- API descriptions, for example as part of the information management model.

BENEFITS

- Describing the API from the perspectives of different architectures helps the organisation understand the significance of APIs to its own operations, datasets, information systems and information flows, as well as to the technologies it is using.
- Linking the API to information, a dataset or a data group is especially important, because the classification of the data processed by the API helps the organisation gain a better understanding of the risks caused and information security measures required by the API.
- A controlled system of APIs improves the reusability, interoperability, information security and data protection of APIs.

SUPPORT MATERIALS

Also see the following materials for help with understanding and describing the enterprise architecture and information management model:

- The Information Management Board's Recommendation for an information management model[59].
- eOppiva training module: Johdanto kokonaisarkkitehtuuriin (Introduction to enterprise architecture, in Finnish)[60].
- eOppiva training module: Kokonaisarkkitehtuurin mallintaminen (Enterprise architecture modelling, in Finnish)[61].

59 The Information Management Board's Recommendation for an information management model (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:29)

60 Johdanto kokonaisarkkitehtuuriin (eOppiva, 2021a)

61 Kokonaisarkkitehtuurin mallintaminen (eOppiva, 2021b)

Principle 2.4 Identify and manage risks related to APIs

Define and adopt a method for identifying risks and threats related to APIs, and for the implementation and monitoring of risk management measures. Include risk management measures in the functional and non-functional requirements for APIs.

Use the risk management instructions[62] drawn up by the Digital Security Steering Committee VAHTI and the organisation's existing risk management processes. Here is an example of how a risk management process can proceed:

- Choose the API or service consisting of several APIs for risk management.
- Identify the data and functionalities processed by the APIs, as well as their classification and administrators.
- Determine how critical the APIs are for the organisation's operations and the factors related to this, such as provisions for continuity and recovery. Also identify the dependencies related to the operation of the API and their potential multiplicative effects.
- Identify the threats and risks related to the API and the information or functionality processed by it. Also take into account risks related to service provision and service levels.
- Prioritise known risks and define management measures for them.
- Define implementation and monitoring responsibilities for risk management measures, along with other possible measures, such as drawing up or updating continuity or disaster recovery plans for APIs.

Take into account the statutory requirements for data processing when planning information security measures. Classified information must be processed according to the handling instructions for classified documents[63], confidential communications must be secured in accordance with the Information Society Code[64], and the protection of personal data in APIs is provided for in the General Data Protection Regulation[65] and Data Protection Act[66].

62 VAHTI risk management instructions (in Finnish) (Digi- ja väestötietovirasto, 2021a)

63 Recommendation on the handling of classified documents (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:19)

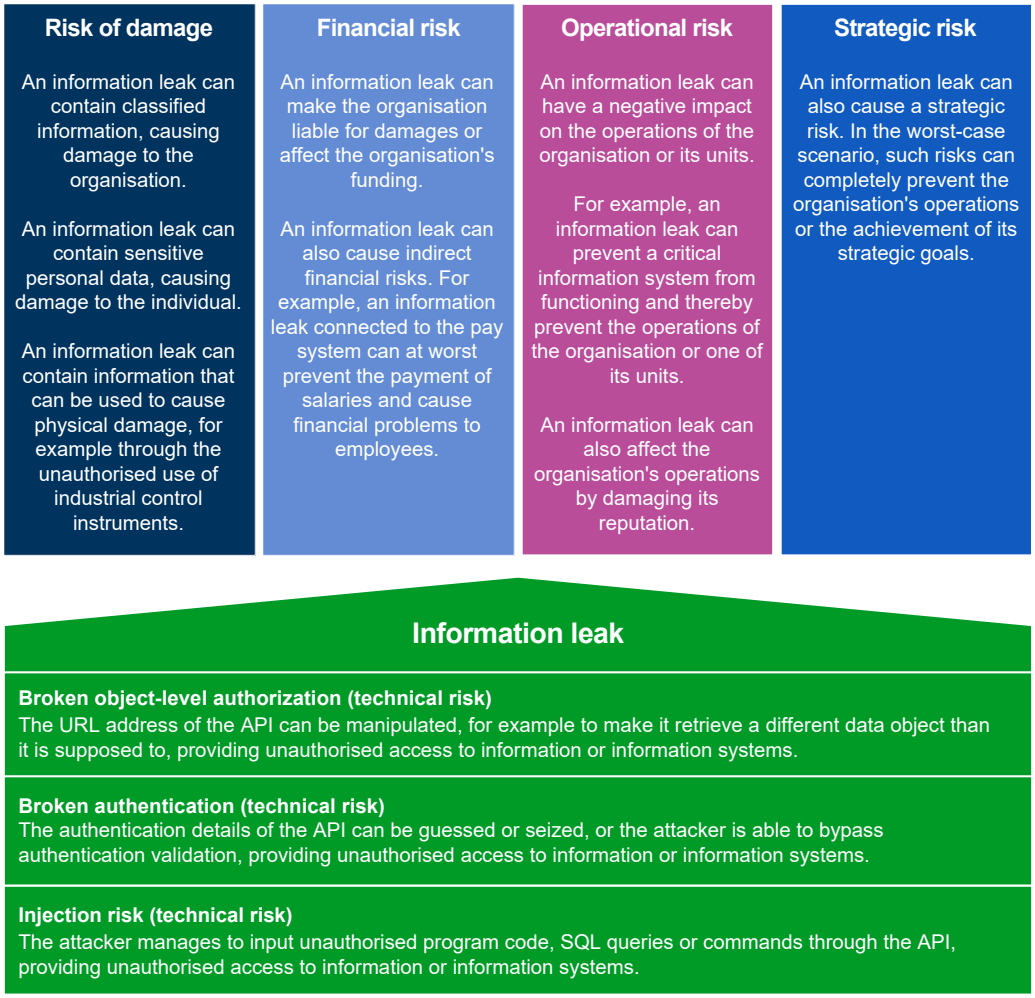
64 Information Society Code (Laki sähköisen viestinnän palveluista 7.11.2014/917, 2014), also see the National Cyber Security Centre's Confidential communications website (Kyberturvallisuuskeskus, 2021b)

65 General Data Protection Regulation (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 2016/679)

66 Data Protection Act (Tietosuojalaki , 5.12.2018/1050)

Also note that the risks related to APIs may have repercussions on other risks identified at different levels of risk management in the organisation. Figure 9 provides an example of how three different risks on the OWASP API Top 10 risk list[67] can cause an information leak, potentially escalating a technical risk to a damage risk, financial risk, operative risk or strategic risk. This is why the effect of the identified threats and risks on the organisation's operations should also be taken into account in API risk management.

Figure 9. Examples of risk posed by APIs.



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

OUTPUTS

- Risk register of the risks caused by APIs.
- Risk management measures for APIs, including measures related to continuity and recovery.

BENEFITS

- By identifying and managing the risks related to APIs, the organisation can minimise the risks and detrimental effects caused by APIs to operations or their continuity.
- Risk management improves the information security and data protection of APIs.

SUPPORT MATERIALS

The following materials can be of help in identifying and managing risks related to APIs:

- Information Management Board's collection of recommendations on the application of certain information security regulations[68], containing a description of information risk management.
- VAHTI risk management instructions (in Finnish)[69].
- The example of API risk management with information risk analysis in Annex 1.
- OWASP API Security Top 10 list[70], containing the most common risks to APIs and measures for their management.
- The National Cyber Security Centre's Secure Development – Towards Approval guide[71], which contains best practices for avoiding vulnerabilities and other common problems in software development.
- Zero Trust Architecture[72], which includes a description of the zero trust model.

68 Collection of recommendations on the application of certain information security regulations (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:65)

69 VAHTI risk management instructions (in Finnish) (Digi- ja väestötietovirasto, 2021a)

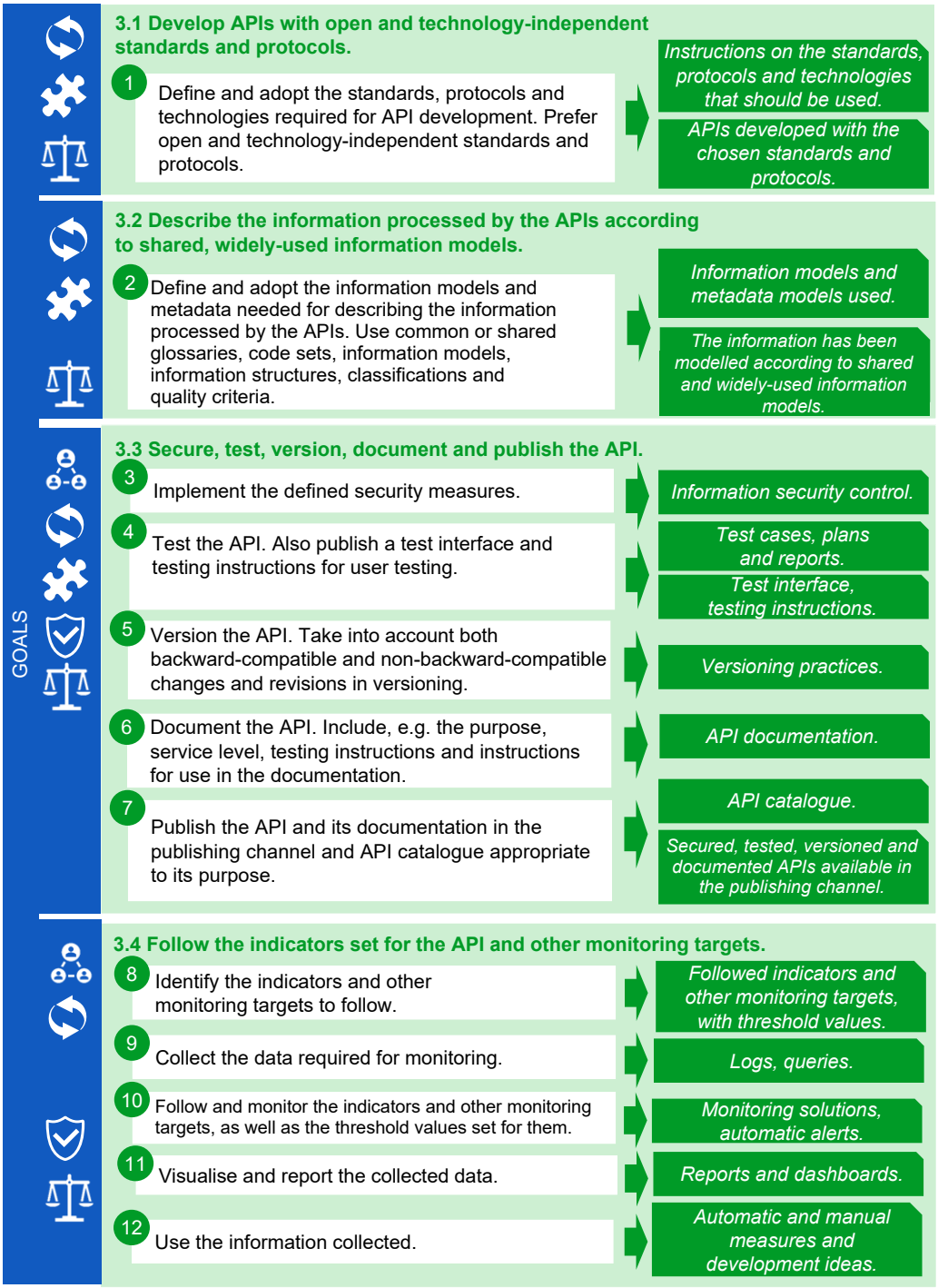
70 OWASP API Security Top 10 2019 The ten most critical API security risks (OWASP, 2019)

71 The National Cyber Security Centre's Secure Development – Towards Approval guide (Kyberturvallisuuskeskus, 2020)

72 Zero Trust Architecture (NIST, 2020)

3.3 Operative level

Figure 10. Operative principles.



Principle 3.1 Develop APIs with open and technology-independent standards and protocols

Define the standards, protocols and technologies required for API development. These are some of the requirements for API development:

- **A data transfer protocol** which specifies how data can be imported or retrieved through the API. **Use of open, widely used and technology-independent data transfer protocols is recommended for APIs.**
- **A file format** which defines the format in which the data processed by the API is described. The file format must be machine-readable. The file format can be based on an open or sector-specific standard or notation.
- **Protocols and methods related to information security** which can be used to implement features such as encryption and access management.
- **Sector-specific standards** which define the nationally or internationally recognised shared practices for a specific sector.

Specify the data transfer protocols, file formats, and security standards, protocols and methods related to data content or information used in the organisation. **Prefer open, modern, widely used and technology-independent standards and protocols**. Take into account the development of both internal APIs and external APIs (partner API, public API) in the specifications.

Prepare the specifications in compliance with sector-specific standards and guidelines, along with statutory or other obligations, which set requirements or restrictions on accepted standards and protocols. For example, the Act on joint support services for electronic government services (Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista)[73] requires the use of the Suomi.fi service channel in certain situations[74]. APIs subject to the requirement must be developed with standards or protocols supported by the Suomi.fi service channel.

Also remember that the information security protocols or methods used must enable the information security measures specified by risk management to be taken, that is, they must be chosen on the basis of the specified information security measures. Information security measures are determined, for example according to the classification of the data processed by the API.

Use the chosen standards, protocols and technologies in your API development.

---

73 Act on joint support services for electronic government services (Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista), sections 3 and 5 (Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista, 571/2016)

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

OUTPUTS

- Instructions on the standards, protocols and technologies to use in API development.
- APIs developed with the chosen standards and protocols.

BENEFITS

- The efficiency of API development is improved and competence requirements reduced when competence is concentrated on the chosen standards, protocols and technologies.
- The use of open and widely used standards, protocols and technologies improves the reusability and technical interoperability of APIs.
- Concentrating competencies on the chosen standards, protocols and technologies improves API quality.

SUPPORT MATERIALS

Examples and additional information on data transfer protocols:

- Web-based APIs normally use an HTTP-based data transfer protocol or architecture model, such as SOAP[75], REST (Representational State Transfer)[76] or GraphQL[77]. Web-based interfaces can be used in both internal and external APIs, and a wide variety of information security controls is available for them. Web-based interfaces enable the real-time synchronous or asynchronous[78] **use of data and functionalities. Data and functionalities should be provided through web-based interfaces if possible and appropriate to the purpose of the API. Synchronous or asynchronous use must be specified based on the needs and requirements set for the APIs.**
- File-based APIs usually use a file-based protocol, such as FTP, SFTP or FTPS. HTTP-based protocols can also be used for providing or receiving files. File-based APIs can be used in both internal and external APIs. Sufficient information security controls must be ensured for external APIs. File-based APIs are a good choice if the information or functionalities are not required in real time, or the data transferred through the API is in file format, such as images, videos or Excel spreadsheets.
- Database APIs normally use a database protocol, such as ODBC or JDBC[79], which lets other information systems, applications or programs open a connection to the database and perform operations there. Database APIs are only recommended for internal use. For example, a database API can be used to collect data into a centralised databank with an ETL integration[80]. If information must be provided to external parties from the information resource, another type of API, such as web-based, is required between the information resource and external actor.

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)

Examples and additional information on file formats:

- Web-based interfaces usually use XML[81] or JSON[82]. XML messages can be described with an XML schema[83] and JSON messages with a JSON schema[84].
- Practically any file format is possible for file-based APIs, including image files (.jpg, .gif, .png), video files (.mp4, .avi) or spreadsheets (.xslx, .csv).
- In a database API, the file format is normally a structure defined by the database, possibly based on the view, table, procedure or other database script.

Examples and additional information on protocols and methods related to information security:

- The most common methods of encrypting data and data communications in APIs are the HTTPS[85] data transfer and TLS[86] encryption protocols. In addition to encryption, external APIs such as partner APIs can use VPN (Virtual Private Network) technologies to create a tunnelled connection between the service provider and user. When processing classified data, the encryption must comply with the National Cyber Security Centre's cryptographic requirements for confidentiality[87] (in Finnish).
- APIs can make use of features such as Basic or Bearer authentication enabled by the HTTP(S) protocol, API-key-based authentication, or the OAuth protocol or versions or certificates derived from it. The authentication mechanism must be chosen according to the risk assessment.
- Also see the National Cyber Security Centre's guidelines on electronic identification[88] and the Digital and Population Data Services Agency's Identification and e-Authorization services[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 National Cyber Security Centre's cryptographic requirements for confidentiality (Kyberturvallisuuskeskus, 2021a)

88 National Cyber Security Centre, electronic identification (Kyberturvallisuuskeskus, 2021c)

89 Identification and e-Authorization services (Digi- ja väestötietovirasto, 2021c), (Digi- ja väestötietovirasto, 2021d)

Examples of sector-specific standards and guidelines:

- Standards and recommendations for geographic information[90] (in Finnish).
- API chart for social services and health care integrations and information systems[91] (in Finnish).
- The national and international standards prepared by the standardisation groups of the Finnish Standards Association[92] (in Finnish).
- Standards applied to the FINNA search consortium, Kulttuuriaineisto-PAS digital preservation service and other joint systems of libraries, archives and museums, such as the FINTO ontology service[93] (in Finnish).
- File formats accepted for preservation and transfer by the national digital preservation service[94]

Principle 3.2 Describe the information processed by the APIs according to shared, widely-used information models

Define and adopt the information models and metadata needed for describing the information processed by the APIs. Use common or shared glossaries, code sets, information models, information structures, classifications and quality criteria[95]. According to the Information Management Board's recommendation, the glossaries used should be based on concepts provided for in law, which should not be redefined or used with other contents. The definition of glossaries is governed by section 2, subsection 3 of the Constitution of Finland, according to which the law shall be strictly observed in all public activity. When a concept is defined in law, it restricts the use of the concept by the authorities[96].

90 Standards and recommendations for geographic information (Maanmittauslaitos, 2021a)

91 API chart (HL7 Finland, 2021)

92 Standardisation groups (Suomen standardisoimisliitto SFS Ry, 2021a)

93 Digime standard portfolio (Digime-tietoarkkitehtuuriryhmä, 2021)

94 File formats accepted for preservation and transfer (CSC – Tieteen tietotekniikan keskus Oy, 2021)

95 Information Management Board's Recommendation concerning technical interfaces and viewing access, p. 11 (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:21)

96 For additional information, see the Information Management Board's Recommendation concerning technical interfaces and viewing access (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:21)

OUTPUTS

- Guidelines for the use of shared and widely used information models and metadata models to describe information.
- The information processed by APIs has been modelled according to shared and widely-used information models.

BENEFITS

- Modelling data processed by APIs becomes easier and more efficient when organisations can use existing information models, data models, code sets and glossaries instead of having to reinvent them every time.
- Shared information models, metadata models, code sets and glossaries improve the reusability, semantic interoperability and quality of APIs.

SUPPORT MATERIALS

Some support materials that can be helpful for identifying shared and widely used information models, metadata models, glossaries and code sets:

- The interoperability platform and interoperability method[97], which includes tools for the specification of interoperable information content.
- Statistics Finland's quality criteria and indicators for information[98] (in Finnish) contains guidelines for describing and assessing dataset quality.
- The Interoperability in Municipalities video published by the Association of Finnish Municipalities[99] (in Finnish) provides additional information on interoperability in municipalities.
- Finto.fi[100], a centralised service for interoperable glossaries, ontologies and classifications from various fields.

97 Interoperability platform and interoperability method (Digi- ja väestötietovirasto, 2021e)

98 Dataset quality criteria and indicators (Tilastokeskus, 2021)

99 Interoperability in Municipalities video (Kuntaliitto, 2021)

100 Finto.fi – a centralised service for interoperable glossaries, ontologies and classifications from various fields (Kansalliskirjasto, 2021)

Principle 3.3 Secure, test, version, document and publish the APIs

Secure the API. Implement the security measures defined in risk management.

Test the API. Define test cases for testing functional and non-functional API requirements, such as usability, fault tolerance, information security and performance. Carry out all testing phases: unit, integration, system, acceptance and regression testing. Use automation for testing where possible. **Also publish a free test version of the API with testing instructions for user testing.**

Version the API. Publish both backward-compatible and non-backward-compatible changes and patches in versioning. Also implement support for several API versions simultaneously if required.

Document the API. Required contents of the documentation:

- Purpose: What are the API and the information or functionalities provided by it intended for? What limitations or restrictions apply to its use?
- Licensing: How are the API and the information or functionalities provided by it licensed?
- Location: Where is the API located?
- API service level or proposition: What is the service level or service proposition of the API? If there is no service level or proposition, for example if the API is still in the trial phase, record this in the documentation.
- Testing and deployment instructions: How can the users of the API test it? How can the users deploy the API?
- Operations or methods offered by the API: What operations or methods does the interface provide? What are the purposes of the individual operations or methods?
- Request and response messages for the operations or methods of the API: What is the structure of the request and response messages? What fields do they contain? What are the data types in the fields and the possible limits on their information content? What kind of values do the fields contain? What do the values mean? Explain the significance of any foreign keys or code set values in particular.
- Possible error codes returned by the operations or methods of the API and their explanations: What error codes can the API return? What do the error codes mean? How should the user react to each error code?
- Contact details of the person or entity responsible for the API: Who can the user contact and how if they have questions, problems or additional needs related to the API?

If possible, use tools that generate at least part of the content automatically for preparing the documentation. Store the documentation in the metadata of the API, for example. Obligations for the implementation and maintenance of documentation for APIs developed by external stakeholders, such as service providers, must be included in the cooperation agreements.

Publish the API and its documentation in the publishing channel and API catalogue appropriate to its purpose. The choice of publishing channel depends on the type of API (internal, partner or external), its users and the classification of the data processed by the API. Please also note that legislation may require the use of a specific publishing channel. For example, the Act on joint support services for electronic government services (Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista)[101] requires the use of the Suomi.fi service channel in certain situations[102].

OUTPUTS

- Implementation of information security controls.
- Test cases, testing plans and test reports.
- Test interface and testing instructions.
- Versioning practices.
- API documentation.
- API details published in API catalogue.
- A secure, versioned and documented API that meets the functional and non-functional requirements has been published in the correct publishing channel.

BENEFITS

- By securing and testing its APIs, the organisation can ensure that they operate correctly, that is, fulfil the functional and non-functional requirements set for them.

101 Act on joint support services for electronic government services (Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista), sections 3 and 5 (Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista, 571/2016)

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

- With versioning, documentation and the right choice of publishing channel, the organisation can ensure that the developed APIs are available for deployment and administration.
- Functional and administered APIs improve customer-orientation and cooperation, reusability, interoperability, information security, data protection and quality.

SUPPORT MATERIALS

Some examples of well-documented APIs that also enable user testing:

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

Additional material related to testing that can be of help in planning API tests:

- API testing instructions, also contain examples of tools used for API testing[105].
- Other system testing instructions, such as the W3Schools Software Testing Tutorial Library[106] or Software Testing Fundamentals[107].
- The DevOps testing instructions[108] published by the DevOps Institute contain a continuous testing model.

Additional material related to versioning, which can be helpful for defining versioning practices:

- Semantic versioning[109].

103 Traficom Open 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 Software Testing Fundamentals (Software Testing Fundamentals, 2021)
108 DevOps Testing (Hornbeek, 2021)
109 Semantic Versioning 2.0.0 (Preston-Werner, 2021)

Additional material related to documentation, which can be helpful for defining documentation practices:

- See the Open API Initiative's Open API Specification[110] and RAML[111] specifications.
- Several API management tools include automatic API documentation, which should be used. Examples of API management tools can be found on Gartner's peer review website[112], for instance. Separate tools are also available, such as Swagger UI[113].

Examples of public API publishing channels:

- The Service Information Resource and avoindata.fi[114].

Examples of partner API publishing channels:

- The Suomi.fi service channel[115] in accordance with the statutory obligation[116].
- VIA integration platform for data exchanges between government organisations[117].
- APIs that process classified data are published in the gateway solution[118] meeting the classification requirements, and the documentation related to such APIs is stored in storage location[119] specified in the classification requirements.
- Other sector- or organisation-specific publishing channels may exist in addition to these.

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 The Service Information Resource (Digi- ja väestötietovirasto, 2022a), Avoindata.fi service (Digi- ja väestötietovirasto 2022b).

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

116 Act on joint support services for electronic government services (Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista), sections 3 and 5 (Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista, 571/2016)

117 Valtori integration services (Valtori, 2021)

118 Gateway instructions (Kyberturvallisuuskeskus, 2021)

119 Recommendation on the handling of classified documents (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:19)

Examples of internal API publishing channels:

- An internal publication channel specified by the organisation. The channel can be some type of API Gateway[120] or other product, or a proprietary solution through which internal APIs can be found and used.

Principle 3.4 Follow the indicators set for the API and other monitoring targets

1. **Identify the indicators and other monitoring targets to follow.** Indicators and other monitoring targets can be derived from the goals set for the operations and from the functional and non-functional requirements set for APIs (see principle 1.2). Indicators and other monitoring targets can be defined and followed at the strategic, tactical and operative levels. Setting permitted threshold values or expected values and a monitoring frequency for the identified indicators and other monitoring targets is recommended. Some indicators or other monitoring targets can be followed continuously in real time, while others are checked at specific intervals, such as every week, month or year. You should also specify how you will react if an indicator goes over or under a threshold value or expected value. For example, what will be done if the load on the API exceeds the threshold values or if the utilisation rate of an API falls short of expectations.

2. **Collect the data required for monitoring.** Data can be collected with various logs or queries, for example. If collecting personal data for monitoring purposes, the requirements imposed by the GDPR[121] and Data Protection Act[122] on its processing must be complied with. If the data collected for monitoring is classified, it must be processed according to the handling instructions for classified documents[123].

3. **Follow and monitor the indicators and other monitoring targets**, as well as the threshold values set for them. Monitoring can be conducted automatically with various surveillance or monitoring solutions, or manually with reports generated at certain intervals. Many monitoring solutions also include a functionality for automatic alerts when a threshold value is exceeded or undercut.

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

121 General Data Protection Regulation (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 2016/679)

122 Data Protection Act (Tietosuojalaki, 5.12.2018/1050)

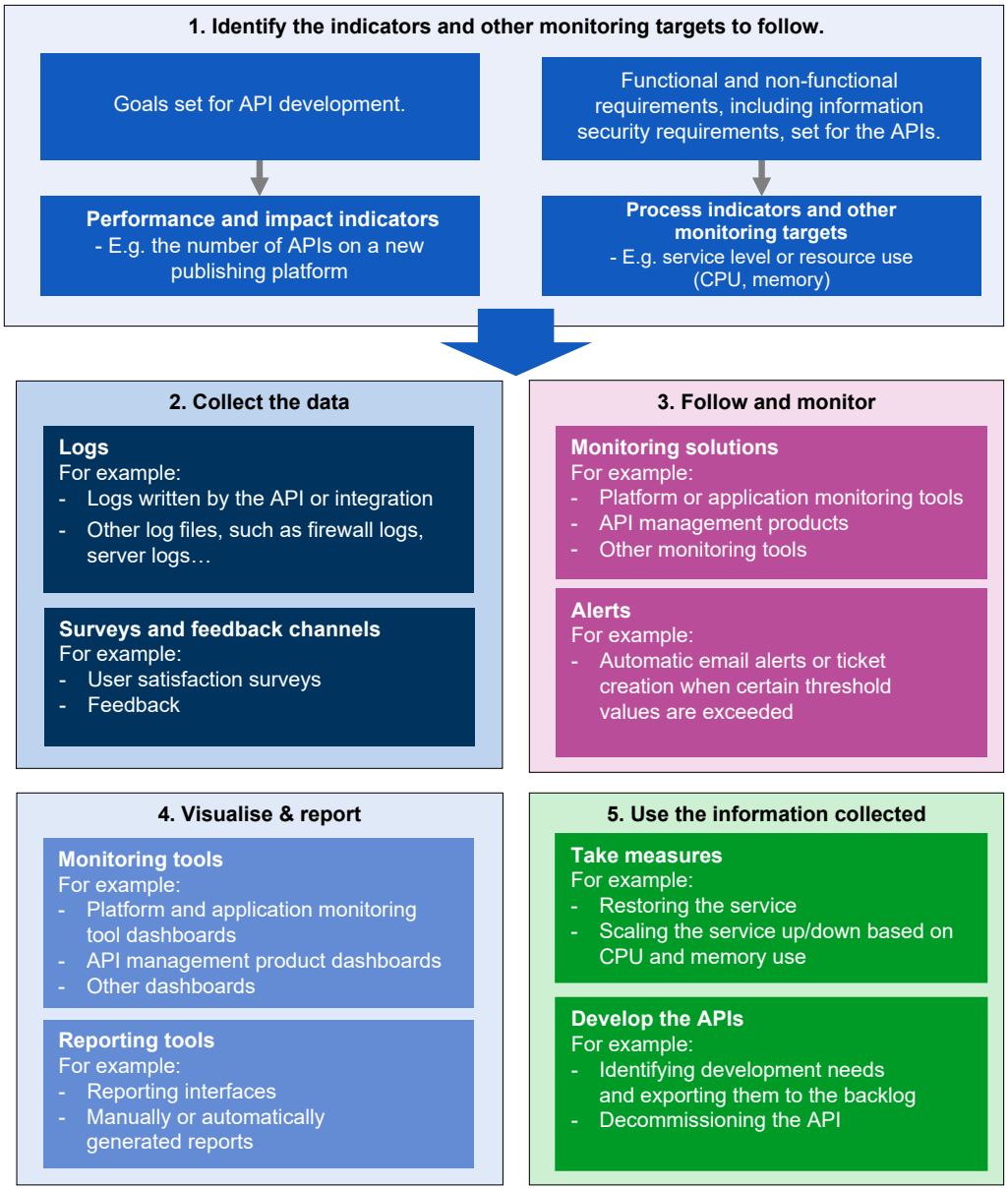
123 Recommendation on the handling of classified documents (Valtiovarainministeriö, Tiedonhallintalautakunta, 2020:19)

4. **Visualise and report the data collected.** Visualisation can be done with various monitoring or surveillance tools, or with reporting solutions or reports.

5. **Use the information collected to identify and take the necessary measures, and for the development or decommissioning of APIs.** Information can be used and measures taken at all levels of the organisation. At the operative level, the monitoring results can be used to identify development needs or development areas related to individual APIs or take measures during production use, such as restoring the API if it has crashed or scaling the API according to its load. Use automation for these measures where possible. At the tactical level, the results of monitoring can be used to identify general development needs, for example relating to the functionalities or non-functionalities of APIs, such as use, usability, information security or the developer experience. Data collected at the strategic level can be used in decision-making related to the development of operations and for monitoring the achievement of goals.

Figure 11 provides a visual representation of the tasks related to API monitoring and examples of the various subjects, such as logs and feedback channels.

Figure 11. API monitoring.



OUTPUTS

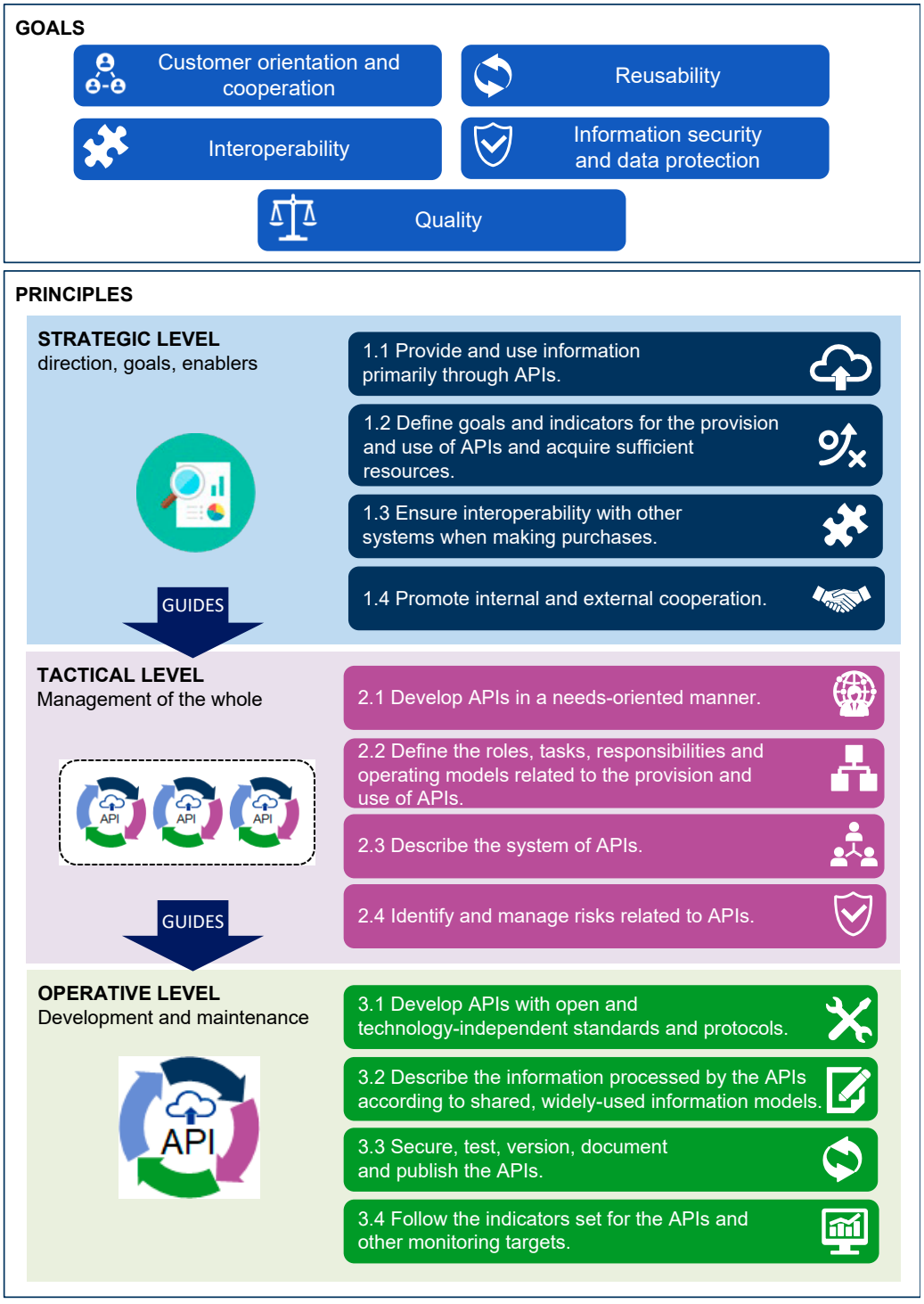
- List of followed indicators and other monitoring targets, with threshold values.
- API and integration log files and other log files, such as server or firewall logs.
- Surveys and feedback channels.
- Monitoring and surveillance solutions.
- Automated alerts.
- Various dashboards or reports.
- Automatic or manual measures and instructions.
- Development ideas/needs, including the need to decommission an API.

BENEFITS

- By following the indicators and other monitoring targets set for APIs, the organisation can verify whether the APIs are functioning as intended and whether the non-functional requirements set for the APIs, such as service level, information security or usability are fulfilled.
- The organisation can also use the monitoring results to verify whether or not its strategic goals have been met.
- Monitoring improves the customer-orientation and cooperation, reusability, information security, data protection and quality of APIs.

3.4 Summary of the principles

Figure 12. Summary of the principles.



SOURCES

Preston-Werner, Tom. 2021. Semantic Versioning 2.0.0. [Online] 2021. [Cited: 21 6 2021.] https://semver.org/.
6Aika-kaupungit. 2016. Palauterajapinta, 6Aika. [Online] 2016. [Cited: 12 11 2021.] https://github.com/6aika/api-palaute.
APIOps Cycles TM. 2021. APIOps Cycles for Lean API Development. [Online] 2021. [Cited: 16 6 2021.] https://www.apiopscycles.com/.
CSC – Tieteen tietotekniikan keskus Oy. 2021. Säilytys- ja siirtokelpoiset tiedostomuodot. [Online] 2021. [Cited: 27 10 2021.] https://www.digitalpreservation.fi/specifications/fileformats.
Department of Defence, United States of America. 2021. DoD Enterprise DevSecOps Fundamentals. [Online] 2021. [Cited: 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. [Cited: 23 8 2021.] https://devops.com/.
DevSecOps. 2021. Manifesto. [Online] 2021. [Cited: 5 8 2021.] https://www.devsecops.org/.
Digi- ja väestötietovirasto. 2021a. Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI. [Online] 2021a. [Cited: 21 6 2021.] https://dvv.fi/vahti.
—. 2021b. Suomi.fi-palveluväylä. [Online] 2021b. [Cited: 23 8 2021.] https://www.suomi.fi/palvelut/suomi-fi-palveluvayla-digi-ja-vaestotietovirasto/4ab88971-b9fb-443c-99aa-bc361bac7548.
—. 2021c. Tunnistus. [Online] 2021c. [Cited: 5 8 2021.] https://dvv.fi/tunnistus.
—. 2021d. Valtuudet. [Online] 2021d. [Cited: 5 8 2021.] https://dvv.fi/valtuudet.
—. 2021e. Yhteentoimivuusalusta. [Online] 2021e. [Cited: 21 6 2021.] https://dvv.fi/yhteentoimivuusalusta.
—. 2022a. Palvelutietovaranto. [Online] 2022a. [Cited: 17 2 2022.] https://dvv.fi/palvelutietovaranto.
—. 2022b. Avoindata.fi -palvelu. [Online] 2022b. [Cited: 17 2 2022.] https://www.avoindata.fi/.
Digime-tietoarkkitehtuuriryhmä. 2021. Digime-standardisalkku. [Online] 2021. [Cited: 27 10 2021.] https://www.doria.fi/handle/10024/180685.
Digitaalinen Helsinki. 2021. Helsingin datastrategia. [Online] 2021. [Cited: 17 6 2021.] https://digi.hel.fi/esittely/helsinki-datastrategia/.
eOppiva. 2021a. Johdanto kokonaisarkkitehtuuriin. [Online] 2021a. [Cited: 21 6 2021.] https://www.eoppiva.fi/kurssit/johdanto-kokonaisarkkitehtuuriin/#/.
—. 2021b. Kokonaisarkkitehtuurin mallintaminen. [Online] 2021b. [Cited: 21 6 2021.] https://www.eoppiva.fi/kurssit/kokonaisarkkitehtuurin-mallintaminen/#/.
Euroopan Komissio. 2017. Eurooppalaiset yhteentoimivuusperiaatteet – täytäntöönpanostrategia. [Online] 2017. [Cited: 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. [Cited: 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. [Cited: 23 8 2021.] https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A32007L0002.
Fintraffic. 2021. Liikenteen avoin data ja rajapinnat. [Online] 2021. [Cited: 19 10 2021.] https://www.digitraffic.fi/.
Gartner. 2021. Full Life Cycle API Management Reviews and Ratings. [Online] 2021. [Cited: 21 6 2021.] https://www.gartner.com/reviews/market/full-life-cycle-api-management.
GitHub. 2021. GitHub. [Online] 2021. [Cited: 30 6 2021.] https://github.com/.
GraphQL Foundation. 2021. A query language for your API. [Online] 2021. [Cited: 21 6 2021.] https://graphql.org/.
Hansel. 2021. Yhteishankinnat. [Online] 2021. [Cited: 4 11 2021.] https://www.hansel.fi/yhteishankinnat/.
Helsingin kaupunginkanslia. 2020. Helsingin kaupungin palauterajapinta. [Online] 2020. [Cited: 12 11 2021.] https://www.avoindata.fi/data/fi/dataset/helsingin-kaupungin-palauterajapinta.
HL7 Finland. 2021. Rajapintakartta. [Online] 2021. [Cited: 5 8 2021.] http://www.hl7.fi/hl7-rajapintakartta/.
Honkanen, Mika. 2021. API-Suomi. [Online] 2021. [Cited: 30 6 2021.] https://fi-fi.facebook.com/groups/apisuomi/.
Hornbeek, Marc. 2021. DevOps Testing. [Online] 2021. [Cited: 30 6 2021.] https://devopsinstitute.com/wp-content/uploads/2018/03/DevOps-testing-ebook-online.pdf.

Hyvän Mitta. 2021. Mittareiden valinta. [Online] 2021. [Cited: 4 11 2021.] https://www.hyvanmitta.fi/mita-mitataan/.
IBM. 2020. ETL (Extract, Transform, Load). [Online] 2020. [Cited: 5 11 2021.] https://www.ibm.com/cloud/learn/etl.
ite wiki. 2021. DevOps. [Online] 2021. [Cited: 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. [Cited: 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. [Cited: 21 6 2021.] https://json-schema.org/.
Julkisten hankintojen neuvontayksikkö. 2021. Julkisten hankintojen neuvontayksikkö. [Online] 2021. [Cited: 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. [Cited: 1 11 2021.] https://finto.fi/fi/.
Kansalliskirjasto, Finna. 2021. Finnan avoin rajapinta. [Online] 2021. [Cited: 12 11 2021.] https://www.kiwi.fi/display/Finna/Finnan+avoin+rajapinta.
Kuntaliitto. 2021. Yhteentoimivuustyö kunnissa. [Online] 2021. [Cited: 21 6 2021.] https://www.youtube.com/watch?v=FNNL8K0EBCI.
Kyberturvallisuuskeskus. 2021a. Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat. [Online] 2021a. [Cited: 1 7 2021.] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf.
—. 2021b. Luottamuksellinen viestintä. [Online] 2021b. [Cited: 25 8 2021.] https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/luottamuksellinen-viestinta.
—. 2021. Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista. [Online] 2021. [Cited: 3 2 2021.] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Yhdyskaytavaratkaisuohje.pdf.
—. 2021c. Sähköinen tunnistaminen. [Online] 2021c. [Cited: 1 7 2021.] https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen.
—. 2020. Turvallinen tuotekehitys - kohti hyväksyntää. [Online] 2020. [Cited: 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. [Cited: 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. [Cited: 23 8 2021.] https://www.finlex.fi/fi/laki/alkup/2016/20161397.
Laki paikkatietoinfrastruktuurista 421/2009. 2009. Laki paikkatietoinfrastruktuurista. [Online] 2009. [Cited: 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. [Cited: 25 8 2021.] https://www.finlex.fi/fi/laki/ajantasa/2014/20140917.
Maanmittauslaitos. 2021a. Paikkatietoalan standardit ja suositukset. [Online] 2021a. [Cited: 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. [Cited: 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. [Cited: 27 10 2021.] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.
OECD. 2002. Glossary of statistical terms: Quality - ISO. [Online] 2002. [Cited: 9 6 2021.] https://stats.oecd.org/glossary/detail.asp?ID=5150.
Open API Initiative. 2021. Open API. [Online] 2021. [Cited: 21 6 2021.] https://www.openapis.org.
OWASP Cheat Sheet Series. 2021a. REST Security Cheat Sheet. [Online] 2021a. [Cited: 5 8 2021.] https://cheatsheetseries.owasp.org/cheatsheets/REST_Security_Cheat_Sheet.html#https.
—. 2021b. Transport Layer Protection Cheat Sheet. [Online] 2021b. [Cited: 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. [Cited: 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. [Cited: 1 7 2021.] https://raml.org/.
Rautio, Pasi. 2015. Strategisten tavoitteiden toteutumisen mittaaminen. [Online] 2015. [Cited: 4 11 2021.] https://www.theseus.fi/handle/10024/89635.
Sharma, Nitin and Tutorials Point. 2019. What is the difference between ODBC and JDBC. [Online] 2019. [Cited: 4 11 2021.] https://www.tutorialspoint.com/what-is-the-difference-between-odbc-and-jdbc.
Software Testing Fundamentals. 2021. Sotware Testing Fundamentals. [Online] 2021. [Cited: 30 6 2021.] https://softwaretestingfundamentals.com/.
Software Testing Materials. 2020. A Comprehensive API Testing Guide. [Online] 2020. [Cited: 30 6 2021.] https://www.softwaretestingmaterial.com/api-testing/.
Suomen standardisoimisliitto SFS Ry. 2021a. Standardisointiryhmät. [Online] 2021a. [Cited: 23 8 2021.] https://sfs.fi/osallistu-ja-vaikuta/standardisointiryhmat/?fwp_aihealueet=tieto-ja-viestintatekniikka.
—. 2021b. Tieto- ja viestintätekniikka. [Online] 2021b. [Cited: 23 8 2021.] https://sfs.fi/osallistu-ja-vaikuta/aihealueet/tieto-ja-viestintatekniikka/.
Swagger. 2021. Swagger UI. [Online] 2021. [Cited: 21 6 2021.] https://swagger.io/tools/swagger-ui/.
TechTarget. 2017. synchronous/asynchronous API. [Online] 2017. [Cited: 4 11 2021.] https://whatis.techtarget.com/definition/synchronous-asynchronous-API.
Tiedonhallintalaki 906/2019. 2019. Laki julkisen hallinnon tiedonhallinnasta. [Online] 2019. [Cited: 8 6 2021.] https://www.finlex.fi/fi/laki/alkup/2019/20190906.
TIEKE Tietoyhteiskunna Kehittämiskeskus Ry. 2021. Verkkolaskufoorumi. [Online] 2021. [Cited: 30 6 2021.] https://tieke.fi/palvelut/liiketoimintapalvelut/verkkolaskufoorumi/.
Tietosuojalaki . 5.12.2018/1050. Tietosuojalaki. [Online] 5.12.2018/1050. [Cited: 9 6 2021.] https://www.finlex.fi/fi/laki/ajantasa/2018/20181050.
Tietosuojavaltuutetun toimisto. 2021. Pseudonymisoidut ja anonymisoidut tiedot. [Online] 2021. [Cited: 25 8 2021.] https://tietosuoja.fi/pseudonymisointi-anonymisointi.
Tilastokeskus. 2021. Tietoaineistojen laatukriteerit. [Online] 2021. [Cited: 21 6 2021.] https://www.stat.fi/org/vuosiohjelma/tietoaineistojen-laatukriteerit.html.
Traficom. 2021. Traficom Avoin Data API. [Online] 2021. [Cited: 21 6 2021.] https://opendata.traficom.fi/swagger/ui/index.
Traficom, Kyberturvallisuuskeskus. 2021. (Online) 2021. (Cited 20.1.2022). Tunnisteet ja tietosuoja -anonymisointi ja sen rajat. Opas. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Tunnisteet%20ja%20tietosuoja.pdf. 2021.
Vaccari, L, et al. 2020. Application Programming Interfaces in Governments: Why, what and how. [Online] 2020. [Cited: 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. [Cited: 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. [Cited: 30 6 2021.] https://finlex.fi/fi/laki/alkup/2019/20191101.
Valtiovarainministeriö. 2021a. Tiedon hyödyntäminen ja avaamisen hanke. [Online] 2021a. [Cited: 8 6 2021.] https://vm.fi/tiedon-hyodyntaminen-ja-avaaminen1.
—. 2021b. Tiedon yhteentoimivuus. [Online] 2021b. [Cited: 9 6 2021.] https://vm.fi/tiedon-yhteentoimivuus.
—. 2022. Julkisen hallinnon tiedonhallintakartta tutkihallintoa.fi -palvelussa. [Online] 2022. [Cited: 17 2 2022.] https://www.tutkihallintoa.fi/tiedonhallintakartta/.
Valtiovarainministeriö, Tiedonhallintalautakunta. 2021:21. Suositus teknisistä rajapinnoista ja katseluyhteyksistä. [Online] 2021:21. [Cited: 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. [Cited: 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. [Cited: 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. [Cited: 8 6 2021.] https://vm.fi/suositukset.
—. 2021:65. Valtiovarainministeriön julkaisuja – 2021:65 Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta. [Online] 2021:65. [Cited: 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. [Cited: 21 6 2021.] https://valtori.fi/yhteinen-integraatioalusta-via-julkiset-varmenteet.
Varsinais-Suomen liitto. 2021. Avoimen tiedon verkosto. [Online] 2021. [Cited: 30 6 2021.] https://kumppanuusfoorumi.fi/foorumi/avoimen-tiedon-verkosto/.
Verohallinto. 2019. API-kehittäminen Verolla. [Online] 2019. [Cited: 17 6 2021.] http://131.207.14.19/contentassets/5389e8bf012445db8fb5865ad0fe745e/10.-api-kehitt%C3%A4minen_verolla.pdf.
—. 2021a. Tulorekisterin tekninen rajapinta. [Online] 2021a. [Cited: 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. [Cited: 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. [Cited: 8 6 2021.] https://vayla.fi/vaylista/aineistot/avoindata/rajapinnat.
W3Schools. 2021a. JSON - Introduction. [Online] 2021a. [Cited: 21 6 2021.] https://www.w3schools.com/js/js_json_intro.asp.
—. 2021b. RESTful Web services. [Online] 2021b. [Cited: 21 6 2021.] REST https://www.w3schools.in/restful-web-services/intro/.
—. 2021c. Software Testing Tutorial Library. [Online] 2021c. [Cited: 30 6 2021.] https://www.w3schools.in/software-testing/.
—. 2021d. XML Schema Tutorial. [Online] 2021d. [Cited: 21 6 2021.] https://www.w3schools.com/xml/schema_intro.asp.
—. 2021e. XML Soap. [Online] 2021e. [Cited: 30 6 2021.] https://www.w3schools.com/xml/xml_soap.asp.
—. 2021f. XML Tutorial. [Online] 2021f. [Cited: 21 6 2021.] https://www.w3schools.com/xml/.

Annexes

Annex 1 Example of API risk management with information risk analysis

The Act on Information Management in Public Administration[124] also requires that the material risks to APIs and the data processed by them be determined and information security measures dimensioned in accordance with the risk assessment. The Digital Security Steering Committee (VAHTI) has drawn up risk management guidelines[125], for the enhancement and harmonisation of risk management in public administration. These guidelines can also be used for API-related risk management[126]. The general risk management process is described in the guidelines proper, and Annex 4[127] to the instructions describes risk management standards and good practices.

In its own study related to the deployment of APIs by governments, the European Commission has identified a number of risks related to APIs and methods for managing them[128]. According to the study, APIs cause technical, organisational, legal and financial risks, which must be identified and managed as part of the organisation's other risk management.

The information risk analysis described in Annex 4 of the VAHTI guidelines is provided as an example here. It can be used to assess the API or service entity comprised of several APIs with basic information security concepts and thereby chart the most likely risks and threats and describe their worst-case consequences.

---

124 Act on Information Management in Public Administration, chapter 4, section 13, (Tiedonhallintalaki 906/2019, 2019)

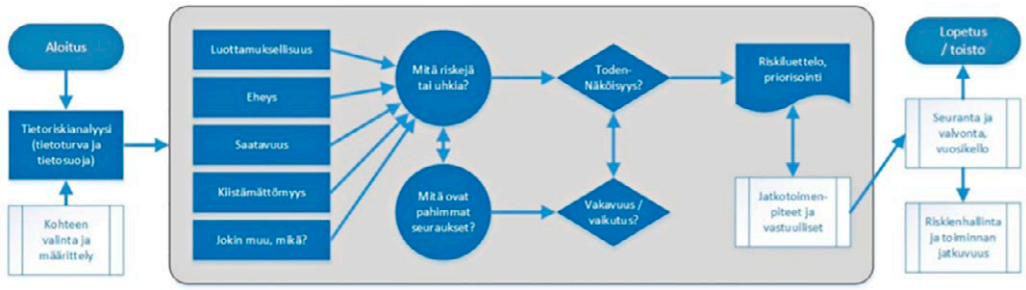
125 VAHTI 22/2017 Risk management guidelines, (Valtiovarainministeriö, VAHTI, 22/2017)

126 Information Management Board's Recommendation concerning technical interfaces and viewing access, p. 16, (Valtiovarainministeriö, Tiedonhallintalautakunta, 2021:21) Katakri 2020 – information security auditing tool for authorities, T-03, p. 11, (Kansallinen turvallisuusviranomainen, Ulkoministeriö, 2020)

127 VAHTI 22/2017 Risk management guidelines – Annex 4, (Valtiovarainministeriö, VAHTI, 22/2017)

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

Figure 13. Information risk analysis after Annex 4 of the VAHTI 22/2017 guidelines.



The information risk analysis begins with choosing an API or service entity consisting of several APIs for analysis and identifying the data processed by them, the classification of the data, and the owners of the data.

The information risk analysis can be carried out by assessing risks and threats targeting the confidentiality, integrity, availability and indisputableness of the data processed by the API. Other risk assessment perspectives include the importance of the API to the organisation's operations, preparedness requirements related to continuity and recovery, as well as internal and external dependencies.

When the perspectives have been chosen, the identified risks or threats related to the APIs are assessed, along with the worst-case consequences should the risk or threat be realised. The probability and severity of the risks thus identified are then assessed, resulting in a prioritised risk list (normally priority = probability x severity).

Finally, risk management measures, the persons responsible for them, and risk monitoring methods and dates are specified for each prioritised risk. Risk management measures can be both administrative (for instance measures related to the development process, such as testing or review practice specifications) and technical (for example implementation of API testing automation and technical information security controls).

MINISTRY
OF FINANCE

MINISTRY OF FINANCE
Snellmaninkatu 1 A
PO BOX 28, 00023 GOVERNMENT
Tel. +358 295 160 01
financeministry.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-367-915-3 (pdf)

February 2022