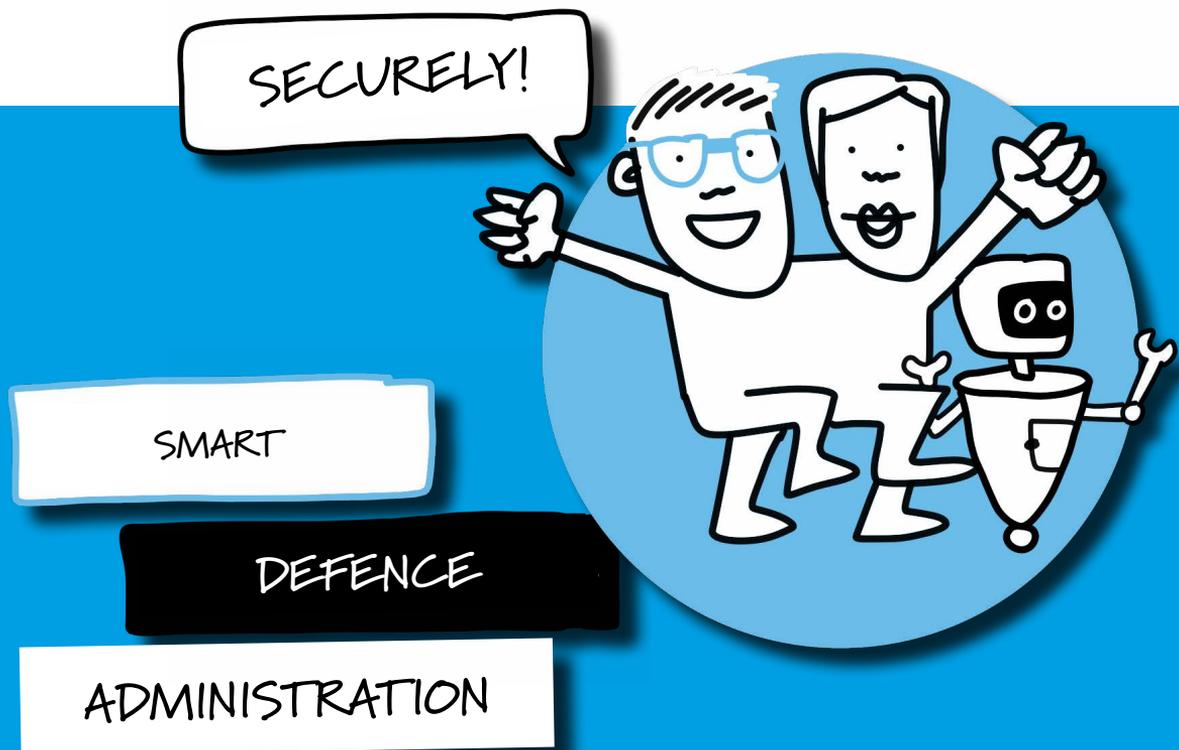


# Securely smart defence administration

## a **DIGITAL CONCEPT**

for the Ministry of Defence's administrative branch



Puolustusministeriö  
Försvarsministeriet  
Ministry of Defence

# CONTENTS

<b>1.</b>	<b>Introduction.....</b>	<b>1</b>
<b>2.</b>	<b>Purpose of the digital concept .....</b>	<b>2</b>
<b>3.</b>	<b>The vision of digitalisation in the defence administration... </b>	<b>3</b>
<b>4.</b>	<b>Implementation plan .....</b>	<b>5</b>
4.1	Specification of operational changes brought about by digitalisation.....	5
4.2	Awareness of opportunities created by digitalisation .....	5
4.3	Understanding the significance of openness .....	6
4.4	Tools, resources and methods to support object achievement.....	6
4.5	Improving interoperability.....	7
4.6	Communication .....	7

Publisher: Ministry of Defence, Finland, 2019  
More information: Aulikki Pakanen, aulikki.pakanen@defmin.fi

ISBN: 978-951-663-064-2 pdf.

Drawings: Linda Saukko-Rauta, Redanredan Oy

# Securely smart defence administration: a digital concept for the Ministry of Defence's administrative branch

## 1. Introduction

Digitalisation is a central theme of Prime Minister Sipilä's Government Programme, and the digitalisation of public services is one of the key projects identified in it. The objective is to leverage the potential of digitalisation to achieve a leap in the productivity of public services while dismantling unnecessary regulation and building a more agile administration. With the help of new operating methods, public services will become user-oriented and primarily digital.

Digitalisation is about a customer-centred change in activities supported by technology. Depending on the technology in question, digitalisation can be categorised in different ways: artificial intelligence, robotics, virtual reality, blockchains etc. Based on the function under scrutiny, it can also be grouped into digitalisation in administration, the customer interface or the operative activities. These aspects are often interlinked. Manifestations of digitalisation include new modes of communication, automation of case management, and the digitalisation of an administrative branch's core functions.

Digitalisation connects branches of government on the one hand, and citizens and the administration on the other. In the course of the work on the concept, dozens of stakeholders were identified, many of whom are also about to go digital. The defence administration needs to digitalise its functions to ensure interoperability with stakeholders. This will also improve efficiency.

Digitalisation is seen as one way of controlling the sustainability gap in public administration. It is estimated that the savings enabled by digitalisation and improved productivity may amount to as much as a billion euros by 2029. The share of digitalisation in central government will be EUR 100 million. In this context, a new model for evaluating the coordination of and investments in digital projects is being prepared.

## 2. Purpose of the digital concept

The digital concept is a tool that will support operating and financial planning and the preparation of performance targets in the administrative branch. It will be used in the strategy work of the Ministry of Defence's administrative branch. The internal digitalisation projects of the agencies in the administrative branch will be described in the agencies' own operating and financial plans, performance targets or other documents.

The digital concept in the Ministry of Defence's administrative branch aims for a phenomenon-based approach to digitalisation. The concept shortly describes how digitalisation will change the activities and what digitalisation looks like from the defence administration's perspective. The defence administration, similarly to all other branches of government, is facing an immense change as new technologies advance at an increasing pace. The objective is understanding the change and developing our competence, making use of digitalisation and preparing for the threats it brings. We are aware of the fact that all impacts of new technologies are not yet known. We acknowledge that questions, also ethical ones, are on the horizon.

Key changes in the operating environment in terms of this concept are digitalisation, the increasing significance of cybersecurity, as well as transparent government and open data. Digitalisation is a driver of change in itself; on the other hand, our environment contains other factors, including those related to efficiency or interoperability, which push us towards digitalisation.

This concept is follow-up on previous documents related to digitalisation in the Ministry of Defence's administrative branch<sup>1</sup>.

---

1 Petra Koivisto: Selvitys puolustushallinnon digitalisaation tilasta, FI.PLM.2017-1819  
Puolustusvoimien digitalisaatiokonsepti, AM16974

Petra Koivisto: Puolustusministeriön hallinnonalan digitalisaation ohjaus, Master's thesis, 2017

Petri Vähäkainu: Teknologinen näkökulma digitalisaatioon, FI.PLM.2017-3533

### 3. The vision of digitalisation in the defence administration

The goal of digitalisation in the defence administration is securely smart defence administration.

This means

- managing the risks associated with new technologies
- optimising current functions
- creating new services, functions and knowledge
- ensuring that investments in technologies create new capabilities
- influencing national-level solutions.

In the defence administration's operating environment, addressing and investigating the cyber threat related to new technologies is vital.

As the operating environment goes digital, the defence administration must tackle both the threats caused by digitalisation and the restrictions digitalisation sets on its activities.

Digitalisation in the operating environment will be taken into account in maintaining, developing and using defence capability and in the improvement of the defence system capability. Digital means will be used to support situational understanding, leadership and rapid decision-making. In the development of capabilities, the potential of digitalisation will be used to maximise effectiveness and impact. Among other things, digitalisation will bring cost-effectiveness, releasing resources for developing and producing other capabilities.

The defence administration will utilise the potential of new technologies in its operations as appropriate. In the selected vision, the defence administration utilises the best practices related to digitalisation and develops competence, however safeguarding information critical for national security and ensuring its integrity and availability. In the vision, stakeholders will interact with the defence administration whenever and wherever they are.

Digitalisation will increase the efficiency of cooperation with other administrative branches. In central government digitalisation projects, uniform methods and tools will have been put in place between the ministries and the agencies subordinate to them. Interauthority cooperation will be based on a common situational understanding, shared information and interoperability supported by digital means. Digitalisation will enable the Defence Forces to support other authorities with the aim of safeguarding the functioning of society in normal and emergency conditions, effectively and with a high impact.

Digitalisation will improve the smooth running and enhance the impact of defence cooperation and promote interaction with partners. Agreements and interoperability at both operational and technical level will enable real-time digital information exchanges. Digital solutions for normal conditions will be used to develop methods for providing and receiving assistance in cases of disturbances and emergency conditions. The planning, preparation and implementation of crisis management operations will be supported by digital means.

The administration of partnerships will be facilitated and their productivity promoted by requiring digital compatibility of the partners. The defence administration will seek partners with an ability to promote digitalisation in the administration. Digital partnerships will facilitate preparedness actions and support security of supply. The defence administration will contribute to promoting the national preconditions for digital industry, with emphasis on developing cybersecurity and cyber defence.

Supported by digitalisation, the turnaround times of defence administration processes will be shortened further. The organisation culture will be open for the opportunities offered by digitalisation. The defence administration will participate in the development and use of the central government's common digital services. The defence administration will disseminate information securely, both internally and to its stakeholders, aiming for openness.

Arrangements for citizens' interactions with the defence administration will be made in keeping with the principles of digitalisation prepared by the Ministry of Finance.

## 4. Implementation plan

The principles of implementing digitalisation in the defence administration:

- Digitalisation will help optimise current functions but also create new services, functions and information.
- The digitalisation of the operating environment will be taken into account in a cross-cutting manner in all activities and continuous improvement.
- The importance of cybersecurity, openness and cooperation will be recognised.
- By renewing practices, user-centred and primarily digital public services will be built.
- Practices will be updated to enable phenomenon-based activities as well as to facilitate smooth life events and business transactions for people and companies.
- The following six areas have been selected for inclusion in the implementation plan. For more detailed actions, see Appendix 1.

### 4.1 Specification of operational changes brought about by digitalisation

For a general description of how the defence administration's operations will be changed by digitalisation, see section 3. All sectors will contribute to formulating a more detailed vision. The defence administration's agencies will put together visions for digitalisation in their sectors. Through its performance guidance, the Ministry of Defence will coordinate the preparation of the agencies' visions and put together the administrative branch's integrated vision. From the vision will be derived the agencies' performance targets for the planning period 2020 and beyond.

### 4.2 Awareness of opportunities created by digitalisation

Technologies are advancing rapidly, and a variety of applications are being introduced both in the public and the private sector. Awareness will be developed through research. However, all the opportunities created by digitalisation are not yet known. Intelligent automation and robotics, for example, remain little used so far.

New types of information can be created by combining data. Digitalisation will be relevant to an increasing number of functions. Competence and knowledge associated with digitalisation will be developed. The defence administration will prepare for the future changes. The point of departure is that the potential of digitalisation will be taken into account in the continuous improvement of activities.

### 4.3 Understanding the significance of openness

“Knowledge is an asset that grows in value when it is shared and processed. The public sector has control of a considerable amount of information resources. Measures that facilitate the use of information resources can increase the value of this intellectual capital, open up opportunities for new business activities, research and education, help develop better services for the citizens, as well as improve decision-making, step up the activities of the administration and make them more transparent.”<sup>2</sup>

Open data and open administration policies have been formulated in many contexts in Finland since 2011. The implementation of Finland’ Open Government III Action Plan began on 1 July 2017. This plan also contains references to open data.

The Ministry of Defence’s administrative branch faces conflicting pressures regarding openness and security. While the general central government policies require openness, the administration is obliged to protect data in the interest of citizens’ safety and security. We need to look at how the central government’s shared projects are compatible with the defence administration’s activities. The defence administration will participate in other administrative branches’ digitalisation projects, ensuring that data critical for security is protected.

### 4.4 Tools, resources and methods to support object achievement

The digitalisation of activities will rely on the best practices and existing principles. The impacts of digitalisation measures on the efficiency and flexibility of activities will be evaluated.

The potential of digitalisation will be taken into account when developing tools. Adequate personnel resources will be ensured. The benefits of digitalisation will be measured more accurately.

---

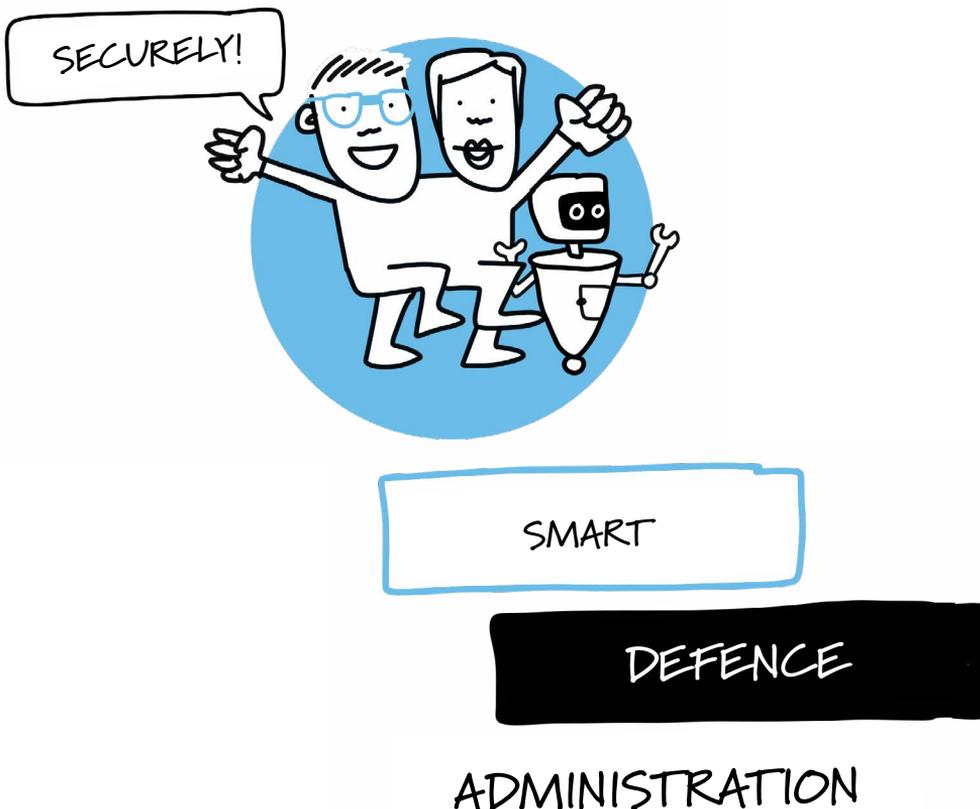
2 Extract from the Ministry of Finance website <http://vm.fi/avoim-tieto>

## 4.5 Improving interoperability

Interoperability is one of the preconditions for digitalisation. Interoperability consists of four layers: legal issues, organisational aspects, semantic concerns and technical challenges<sup>3</sup>. We can exert influence on all of these layers. The problem areas and opportunities of interoperability will be identified at all levels.

## 4.6 Communication

A precondition for the digital concept's success is efficient communication, which also includes information exchanges within the administrative branch on topical issues relevant to digitalisation. Those working with digitalisation in the defence administration and its stakeholders will form a network to support information exchanges and competence.



<sup>3</sup> European Commission: New European Interoperability Framework, [https://ec.europa.eu/isa2/eif\\_en](https://ec.europa.eu/isa2/eif_en)

**TAPPING INTO**  
existing competences &  
**SMOOTHER PERFORMANCE**  
at work  
ACROSS ORGANISATIONAL BORDERS!!