Republic of Estonia
Government Office

Republic of Estonia
Ministry of Justice and Digital Affairs

Co-funded by the European Union
Investing in your future

Selection of owner and provider of a digital service

Guide for the public sector in planning the development of digital services

SPRING 2025

The guide has been prepared at the request of the Government Office and the Ministry of Justice and Digital Affairs to support public sector institutions in the development and planning of digital services. The preparation of the guide was funded by the measure “Strengthening the Innovative Capacity of the Public Sector” of the European Union Cohesion Policy 2021–2027.

The authors of the guide are:
Maari Helilaid
Siim Sikkut
Kristo Vaher
Kati Jakobson-Lott
Veiko Lemberg (TalTech, Ragnar Nurkse Institute)
Külli Taro (TalTech, Ragnar Nurkse Institute)

The team would like to thank everyone who contributed with their knowledge, experience and input: Aivar Hiio, Moonika Schmidt, Anni Lehari, Ott Velsberg, Anne Jürgenson, Urvi Kaljas, Kalev Pihl, Tea Varrak, Märt Aro, Katri Samarütel.

Our special gratitude goes to the Estonian Association of Information Technology and Telecommunications and EdTech Estonia, whose active involvement and cooperation contributed significantly to the preparation of this guide.

Contents

Annexes

Summary

The purpose of this guide is to support public sector service owners in deciding which digital services should be provided by the state itself and which ones may be entrusted to the private sector.

The guide is divided into **three thematic blocks** that help to consider whether and how the state could work with the private sector to provide digital services.

These are:

Assessment of economic efficiency

which helps to think through thecost components of the digital service and assess whether the involvement of the private sector in the provision of the digital service could be more cost-effective than providing the digital service oneself

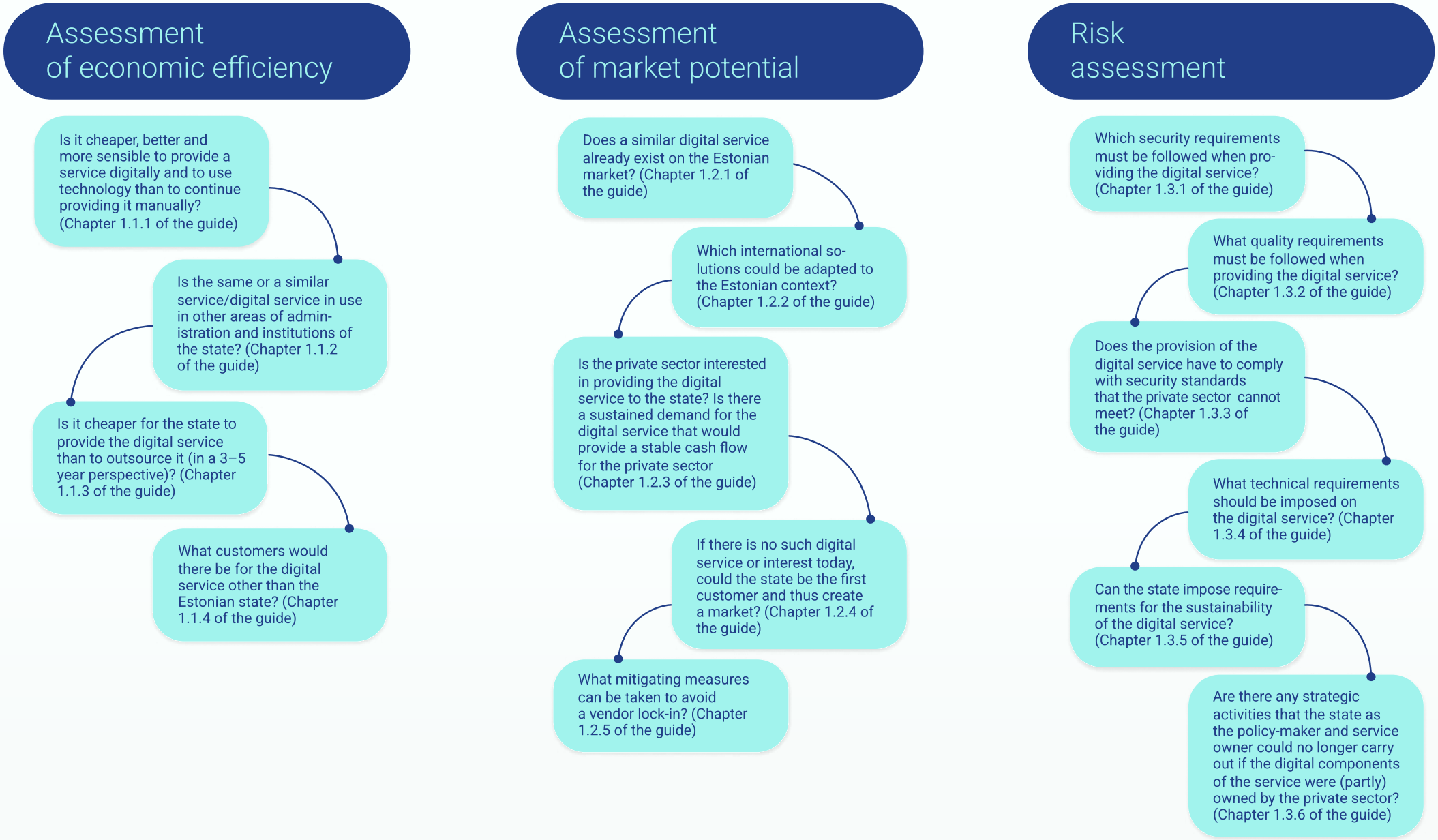
Assessment of market potential

which guides towards analysing market capacity and potential

Risk assessment

which highlights some of the key risk areas and guides towards consideration of mitigating actions

The guide is supported by a simplified decision pathway for digital service owner and provider selection:



Definitions[1]

Service means the result of an activity or activities of the state that creates value for the beneficiary or user. Ser-vices are provided to achieve the state's strategic objectives and to comply with legislation. A beneficiary and a user can also be referred to as a customer.

Digital service means the provision of a service using digital technology. This can mean a user interface, data exchange, application process, self-service, decision made through an information system or any other function that is realised through technological means. A digital service is not a separate type of service, but a way of delivering part of the content or process to the user. Most public services are a combination of digital and non-digital elements – such as human labour, physical presence or administrative activities that are not replaced by technology.

Beneficiary/user/customer means a natural person or legal entity who uses or has expressed interest in usingthe services. The wider public or society in general can also be the beneficiary.

Direct public service means a service provided by an authority to a natural person or a private legal entity at their request, including presumed request, through a service contact by any means of communication, and which enables that person or entity to fulfill a legal obligation or exercise a legal right. For example: access to state pensions, consular services and assistance, issue of activity licenses, etc.

Internal support service means a service that supports the functioning and service provision of one's own institution. For example: human resources management, document management, legislative drafting, warehouse services, management, internal audit, information security.

External support service means a service that supports the functioning and service provision of another institution. For example: payroll and accounting, financial accounting and public procurement services provided by the State Shared Service Centre; services of central IT institutions to centres.

Indirect service means a service where institutions offer a service provided for by law without direct contact with the beneficiaries of the service and where the beneficiaries of the service cannot be identified. The beneficiary is society or a part of society. For example: development of welfare policy and organisation of its implementation, traffic control, prevention, reduction and treatment of alcohol abuse, fire safety inspection service.

Service owner means the person (by their position) who decides on the targeting, budgeting/resources, identification of the target group/interest group and monitoring of the service. As a rule, this is the head of the area and/or department. The service owner themselves may not be involved in the provision of the service, but manages, organises and improves the service according to the results of the service metrics. The Principles for Managing Services and Governing Information require an institution to determine the positions or jobs where the persons employed ensure the organisation and quality of the services and processes of the institution. Although the role of the service owner is in practice linked to a specific individual, this guide also uses the term in a broader sense – considering either the state or the private sector as the service owner, depending on which of them is responsible for the purpose, operation and development of the service. This gives a clearer view of strategic decisions on the organisation of service provision and the allocation of responsibilities.

Digital service owner means an organisation (including an NGO or a company) responsible for providing a digital service or product. The digital service owner may be different from the service owner: the service owner is usually the state, while the owner of the digital service or product by means of which the public service is provided may be the private sector. For example, if the service is a primary health care service, the owner of the GP information system (digital service) may be a private company (e.g. AS Medisoft).

Service privatisation means, in the context of this guide, the process of ownership change whereby ownership of a public service or asset (including software) is transferred from the public sector (local authority or state) to the private sector, including e.g. a private non-profit association. In other words, it is a situation where a service previously provided by the public sector is handed over to the private sector, which will then provide the service either on behalf of the state (i.e. the state buys the service) or directly to residents or companies (i.e. the state is no longer the customer or the funder, but only acts as a regulator or supervisor).

Contractual delegation of a service, or also the authorisation or transfer of an administrative task, means the entrusting of a public service or support function to a private company, an NGO or another public sector organisation for performance. The state itself remains responsible for the service, funds the provision of the service and supervises it.

Outsourcing the service means, in the context of this guide, a situation where the public sector starts using a private sector service or solution by paying a fee to the other party. The ownership rights related to the service/solution will remain with the private sector, with the public sector becoming the contractual customer alongside other market players.

1 Definitions are based on, among others, the Activity-Based Budgeting Manual (Link)

Introduction

The purpose of this guide is to support public sector service owners in deciding which digital services should be provided by the state itself and which ones may be entrusted to the private sector.

The state currently has more than 1,400 digital services, mostly provided by the public sector. However, if we follow the principle of minimalism – that the state intervenes only when absolutely necessary – it is clear that not all digital services need to be provided by the state, nor should they be.

In many cases, the private sector can provide digital services faster, more flexibly and in a more scalable manner, including by enabling their wider uptake outside the public sector and Estonia. In fact, the private sector is often very well-equipped and technically competent in providing digital services – often even more flexible than the national development capacity. Private companies are usually better placed to respond quickly to changing technologies and user expectations. Therefore, there is no reason to assume that digital solutions offered by the private sector are in any way of inferior quality, when often the opposite is true: market competition and specialisation lead to better user experience, more innovative solutions and faster development capacity. The state should not duplicate competences already available on the market, but use them wisely and strategically.

The central question of the guide is: should a particular digital service be provided by the state itself, or would it be more sensible to do it in partnership with the private sector, or to rely entirely on private companies to provide it? In some cases, the analysis may show that the provision of the digital service is not practical at all at the given time and it should be discontinued or redesigned.

Involving the private sector to a greater or lesser extent in service provision does not mean abandoning policy-making in the area. Privatising, outsourcing or involving the private sector in the provision of digital services does not mean that the state waives its responsibility as a policymaker in the area or, more broadly, as the service owner.

Providing digital services and policy-making are two different roles with different objectives and tools. Policymaking means that the state determines what problems need to be solved in an area, what the desired outcomes are, and what values, principles and rules should guide these solutions. This covers legislation, preparation of strategies, setting priorities, impact assessments, etc. – all of which are and will remain the responsibility of the state.

The provision of digital services, on the other hand, is one possible way to achieve political goals – a concrete technical and practical solution. In the case of technological implementation, this can be provided through various forms of cooperation, including with the participation of the private sector. This distinction becomes particularly important in the case of digital solutions, as almost every public service today includes an IT component. Even if the service is provided in a physical environment, such as a service office, it is still based on information systems, databases or other digital solutions. Most services are therefore complex services, which consist of a number of sub-services or activities, some of which are digital, some not. Therefore, the involvement of the private sector in the development and technical implementation of a digital service does not affect the role of the state as a policymaker and, more generally, as the service owner.

Who?

The guide is designed to be used by service owners and public sector decision-makers responsible for making choices about the development of digital services.

When?

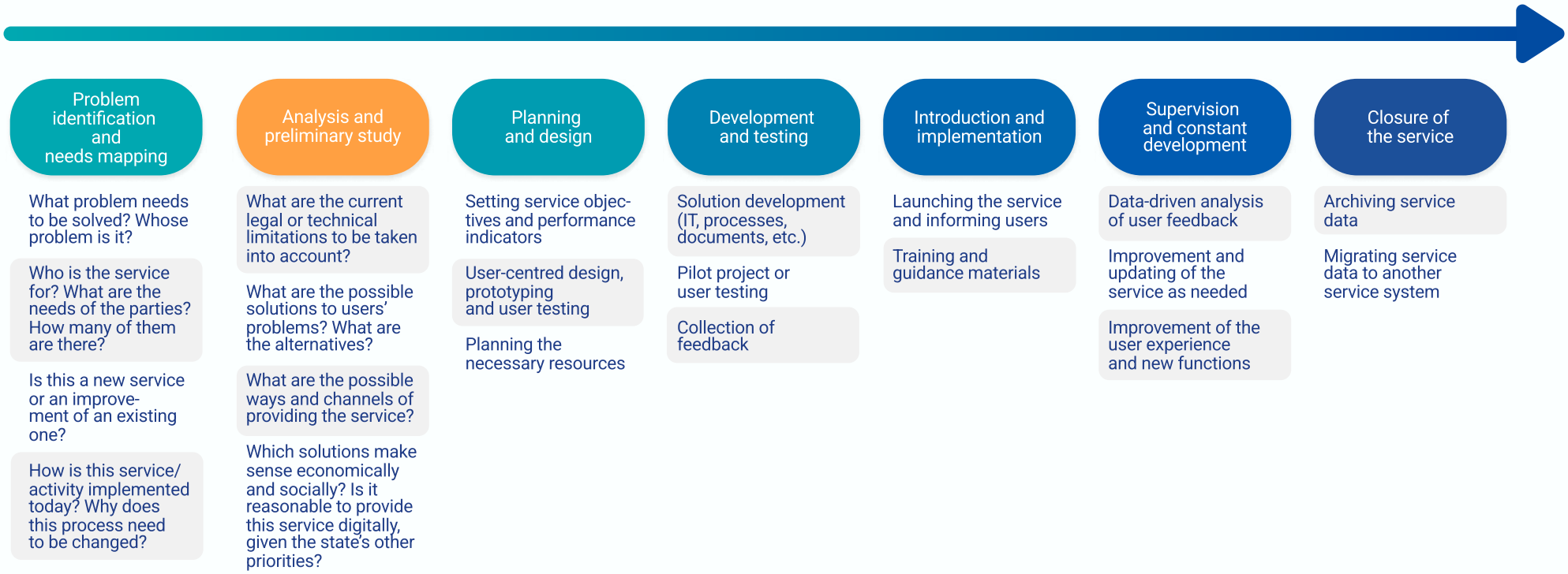
Developing a service is not a one-off activity. For each service, it would be sensible to define the frequency at which the operation of the service will be reviewed and next steps will be decided. Such a review could be prompted by, for example:

- User feedback
- Policy changes
- Planning of the service and its funding needs (RES/RE process, including changes to programmes)
- Expiry of the existing public contract
- New national development trends and their implementation (e.g. event services)

This guide can be used in all of these processes when it is necessary to ensure whether the decisions made so far regarding the provision of the service are still relevant and correct or alternatives should be considered. The guide can be used both when reviewing a service and its provision as a whole, and when assessing the creation or functioning of a digital component or functionality of a service.

Preliminary conditions

A simplified description of the journey of development/introduction of a service in chronological order would look something like this:



The second of these stages, i.e. the stage of analysis and preliminary studies, leads to the question of how or through which channel it would be reasonable to provide the service. If the idea here is that digital solutions should be (one of) the channels for service provision, then that's where this guide comes in to help analyse whether and by whom a given digital service should be provided.

Alternatives

Broadly speaking, there are five types of cooperation in public-private partnerships (including non-governmental organisations), which are often combined in practice:

1 **The public sector provides access** to the necessary inputs for the creation of the (digital) service, but does not intervene in the provision of the (digital) service. An example is the open data of the public sector, where the public sector does not intervene in the creation or provision of services other than through the publication of data. In essence, conditions are created for new (digital) services to emerge without any public sector expectations; there is no direct partnership.

2 **Contractual delegation of a service** (but also authorisation or transfer of an administrative task). This means entrusting a public service or support function to a private company, NGO or another public sector organisation for performance. The transferor of the service defines the nature, scope and/or other essential conditions of the service, generally finances part or all of the provision of the service and supervises the provision of the service.

As a rule, the contractual delegation of a service has been implemented in Estonia as an internal transaction, where public authorities have delegated the provision of a service, either by private or administrative contract, to e.g. a foundation established by the state, a state-owned company or other bodies controlled by the public authority. Examples include the development of the area of entrepreneurship and innovation and the provision of grants by the Estonian Business and Innovation Agency. So far, there are no good practices of the delegation of only digital services in Estonia.

3 **Outsourcing a (digital) service,** where the public sector starts using a (digital) service or solution of the private sector.

It differs from contractual delegation in that the ownership rights related to the service/solution will remain with the private sector, with the public sector becoming the contractual customer alongside other market players. This is a typical involvement of the GovTech sector, which refers to solutions developed and managed by private organisations and intertwined with public sector components (e.g. registries, algorithms, API) to facilitate processes in the public sector[2] . Examples in Estonian practice include Mobile-ID and Smart-ID, as well as Microsoft's digital products, which are privately owned digital services where the state is one customer among many.

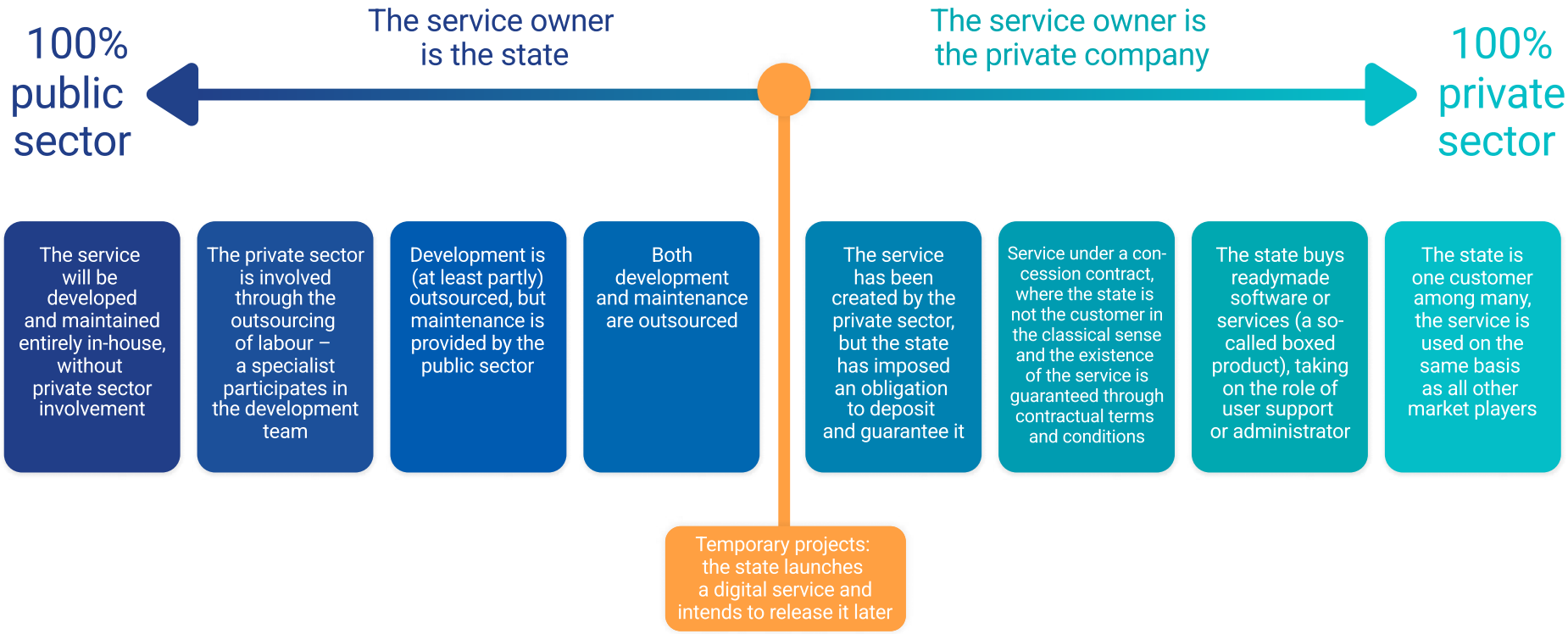
4 **Privatisation of a (digital) service.**

This is a situation where the public sector abandons the provision of a public (digital) service and does not interfere in the user-provider relationship (general regulatory limitations may remain). There is no direct partnership. The providers of the (digital) service are, for example, non-profit associations in the private sector, established in public interests and for a public objective, in whose operations the state may participate, for example in an advisory role. In Estonia, state-owned companies have mostly been privatised (AS Eesti teed, Operail, etc.).

If intellectual property belonging to the state must be transferred to a company for the provision of a (digital) service, it can be done on favourable terms (free of charge or below market price) on the basis of the State Assets Act if this serves a public purpose such as education, health, rescue or social services. It is also possible for the state to transfer the intellectual property necessary for the provision of a (digital) service to a private company operating for commercial purposes, e.g. through a public auction, whereupon the service provider retains the freedom to provide the (digital) service as it sees fit. The amendments to the State Assets Act, which entered into force in 2021, separately describe the process of giving the state's software into use free of charge. If the source code of the relevant public software has been made available to the public free of charge and indefinitely by the state, this means that there is no need to organise a public auction or assignment of property rights, but a private operator can use the relevant software on the basis of a user agreement (licence).

5 **Other forms of partnership** where the public and private sectors jointly contribute their resources to the provision of a (digital) service. For example, through the allocation of targeted or operating support, setting up joint organisations, building common infrastructure, creating common data sharing platforms, or even stimulating innovation through prizes/competitions.

2 Bharosa, N., 2022. The rise of GovTech: Trojan horse or blessing in disguise? A research agenda. Government Information Quarterly, 39(3), p.101692.



The following guide does not focus in detail on the specificities of each form of cooperation, but aims to guide the user to consider the different forms of cooperation with the private sector. **A key issue in the alternatives described is determining the owner of the service and the digital service.** In the situations presented in this guide, as a rule, the state is and will remain the service owner, and the service owner decides how the service is provided (i.e. as a digital or non-digital service). And from there, they decide how to involve the private sector in the provision of the digital service. If the state itself remains the owner of the digital service, it is possible that the digital service will be developed by the private sector, i.e. the development (or parts of it) will be outsourced with a procurement. In a situation where the digital service remains in the ownership of the private sector, the state can intervene in its design, e.g. the public sector can oblige a private sector company to deposit the development code with a notary, or set rules on the provision and termination of the service.

1 Guide

Below is a description of three thematic blocks that will help with considering whether and how the state should work with the private sector to provide digital services. These are:

1. **Assessment of economic efficiency,** which helps to think through the cost components of the digital service and assess whether the involvement of the private sector in the provision of the digital service could be more cost-effective than providing the digital service oneself.
2. **Assessment of market potential,** which guides towards analysing market capacity and potential.
3. **Risk assessment,** which highlights some of the key risk areas and guides towards consideration of mitigating actions.

The general background, recommendations and examples of past practices are described for each of the topics covered. **By the end of the guide, you should be able to answer the questions "Why make this decision?" and "Why are other alternatives not suitable?".**

The guide can be used:

- to carry out the initial assessment of the digital service
- to map which additional activities and analyses should be carried out before making the final decision

Using the guide for the initial assessment of a digital service does not require too much (preliminary) work and outsourcing of extensive analyses. However, it would be a good idea to think through some questions before the assessment (see also "ANNEX 4 Worksheet for preparations: Present description of the digital service"):

1 what problem will the digital service solve?
2 what is the content of the digital service?
3 who are the main users of the (digital) service and how many of them are there (e.g. the average number of users per month or per year)?
4 how much does the provision of the (digital) service cost at present?
5 what are the main risks known today?

Using the guide and completing the assessment of the digital service may lead to the need for more in-depth mapping, which should focus on finding solutions to the problems raised.

1.1 Assessment of economic efficiency

The decision to develop a new digital service or transform an existing digital service should start with weighing its economic efficiency. Before planning or investing in technical solutions, it is important to assess whether the development of a digital service is justified at all – especially in terms of the potential number of users and the cost of providing the existing (e.g. manual) service. The first block of the guide will help the digital service owner make informed decisions by asking thematic guiding questions that help assess the need to develop a digital service and possible alternatives. In addition to the economic justification, the guide also draws attention to other important aspects: whether a similar service is already in use in other public authorities (and could duplication be thus avoided), the cost components of development and management compared to private sector options, and the actual customer base for the digital service.

1.1.1 Is it cheaper, better and more sensible to provide a service digitally and to use technology than to continue providing it manually?

In order to consider whether to provide a digital service oneself or to outsource it, it is important to be clear about what one wants to offer users, what the purpose of the digital service is and what one wants to achieve. In order to answer these questions, it is necessary to consider whether the development of a digital service is reasonable at all, taking into account, for example, the number of users/beneficiaries of the digital service and the cost of providing it manually. In simple terms, the decision to digitise is, of course, an easy one: it only makes sense to digitise a service if it facilitates and reduces the repetitive and automatable routines that exist in the service and measurably improves the quality or efficiency of the process. If development and management are more expensive than the manual provision of the service, the development of a digital service would be a potential waste, so it is important to clearly justify why it is necessary.

Example

A known example of Estonia's digital state being unreasonable relates to the development of a tax credit system for Estonian Olympic champions. Estonia has had 26 Olympic champions throughout history, some of whom have now passed away. The commercial need for the solution created is understandable and reasonable, but the costs of automating the service were higher than paying an accountant to calculate these benefits manually.

Recommendations

1 **Describe the service as simply as possible.** Write down what's happening with the current service: who's doing what, how many steps are involved, how long it all takes, etc. Think: **"Where is a lot of time being spent? Where is the same thing done several times? Where do errors or congestion occur?"** This can also be done as a small discussion with colleagues – the objective is not to have a perfect process map, but to highlight the main "sore points".

2 **Think about the following key questions:**
- Is part of the service repeated in a similar way each time?
- Is data entered manually or several times?
- Do people have to come in or mail paperwork when it could be done online?
- Are there enough users of the service?

If you answered **"yes"** to several questions, you may have reason to believe that the service would be **at least partially** suitable for digitisation.

3 **Make a quick financial comparison:** would the technology bring savings or improve quality?
- Assess whether the number of users of the service is large enough to justify creating a separate digital service.
- Consider how many hours of staff time per month it takes to provide this service today.
- Multiply this by salary and see what the annual cost is.
- Add *ca* 15% to staff costs to cover overheads.
- Then ask your IT centre or a developer for the rough price of the creation of a digital solution.
- If the costs of a digital solution would pay off in a few years and quality/working time would be improved, there is reason to think about digitisation more seriously.

1.1.2 Is the same or a similar service/digital service in use in other areas of administration and institutions of the state?

A suitable digital service may not be only available in the private sec- tor – the necessary functionality may already exist in another public authority. In this case, scaling up and introducing the existing digital service or solution should be considered, rather than starting to develop a separate solution. This does not mean giving up on quality or on the consideration of special needs, but a conscious preference for cooperation, saving resources and reusing proven solutions. A joint development or takeover of an existing digital service can be the fastest and most sustainable way to achieve the desired result, especially if the digital service performs more general support functions – such as document management or user support.

Example

An authority is considering the development of a new procedural environment to support its sectoral administrative proceedings. Looking at the bigger picture reveals that several other public authorities are also engaged in similar procedural processes and are already using digital services that cover much of the desired functionality – such as registration of documents, preparation of decisions, tracking deadlines and data exchange with parties, workflow management, etc. A more in-depth analysis shows that existing procedural systems can be architecturally differentiated to meet the specific needs of the authorities through role management and rights, allowing the use of different procedural logics or workflows within a single system. In this case, instead of creating a new digital service, it may be more sensible to consider extending or adapting the existing solution to reduce duplication, speed up introduction and save resources.

Example

National authentication service TARA. Some time ago, the state developed its own authentication solutions as additions to new digital services, which integrated the functionalities of the ID card and Mobile-ID. The Estonian Information System Authority collated the needs for such solutions and developed the central authentication gateway TARA, which is now used to log in to most Estonian e-services.

Recommendations

1 **Assess** whether the functionality is unique, or whether similar activities exist in other authorities as well.

2 **Consult** with IT centres, the Centre of Registers and Information Systems, the Estonian IT Centre or the Ministry of Justice and Digital Affairs to identify the current practices and digital services used by the other authorities and their possible suitability for the provision of the service.

3 **Contact** colleagues from other authorities doing similar work, e.g. from local authorities, to map their user experience.

1.1.3 Is it cheaper for the state to provide the digital service than to outsource it (in a 3–5 year perspective)?

The analysis of the total cost of a digital service helps with making informed decisions to ensure the most optimal solution, both economically and strategically. While the first control question analysed whether digitisation of the service makes economic sense at all, now the cost of providing the digital service by the state and the private sector should be compared. Regardless of whether the digital service is developed in-house or (partially) outsourced, it is important to take into account all cost categories over the life cycle of the digital service and compare them realistically with possible alternatives. The majority of cost categories apply to both the public authority itself and the private sector.

Example

of how the state does not always take into account the full life-cycle costs of developing digital services: the period when many developments were being financed by external funds, in particular EU grants. The grants made it possible to quickly create new solutions, but often the project budget focused only on the development stage and neglected the future management and maintenance of the digital service. When the grant project came to an end, it was suddenly necessary to find additional funding from the state budget to keep the created solutions functional.

Recommendations

1 In order to thoroughly assess the cost-effectiveness of the provision of a digital service, we recommend starting with a description of the cost types involved in the development and provision of digital services. The following is a typical list of the costs involved in the provision of a digital service, covering the whole service life cycle:

- Staff costs – salary costs, including remuneration, taxes and benefits (e.g. training, bonuses). The state should also take into account the contribution of existing staff in the management and development of the service, as their time is a cost that should be included in the total cost of the service.
- Development and configuration costs – software development, testing, system integration and other initial investments necessary to get the service up and running.
- Infrastructure costs – costs related to the use of servers, databases and cloud services, as well as hardware and network resources.
- Maintenance and management costs – regular updates, ongoing system maintenance, bug fixing and technical support.
- Licences and intellectual property costs – software licences, patents, copyrights or other related fees.
- Security and data protection costs – security audits, compliance checks, data security solutions and legal advice on data protection requirements.
- User support and training costs – training and support for users, including helplines, guidance materials and a user support team.
- Contractual and administrative costs – if the service is outsourced, the costs of contract management, legal advice and risk management must be taken into account, plus the costs of public procurement and supervision on the state's side, and the cost of submitting a tender for the private sector.
- Sustainability and development costs – costs related to the development of new functionalities, system upgrades and technology lifecycle management.

2 Once the cost types have been described, compile a detailed cost calculation in the state's view. Please note that using existing resources (manpower or, for example, the use of existing server space) also comes with associated costs. If you have not previously calculated the existing cost on the basis of digital services, please do so.

3 In order to estimate the costs for the private sector, consult experts from IT centres, the Estonian Information System Authority, the Centre of Registers and Information Systems, etc. if necessary, to identify potential average market prices of the private sector. You can then compare the costs that would be incurred by the state with the costs that would be incurred by the private sector.

4 Please note that the important thing is not to achieve savings in each cost type, but that as a whole, the provision of a digital service today or over a certain period of time (e.g. 3–5 years) should be more efficient when done by the private sector than when done by the state.

1.1.4 What customers would there be for the digital service other than the Estonian state?

When developing a digital service, it should be assessed whether the Estonian state is the only customer or whether it has a wider market potential. If the digital service can also be provided elsewhere – for example, in other countries or in the private sector – this can reduce the state's costs and strengthen the international competitiveness of Estonian technology companies. However, if the state would be the only customer, it must be taken into account that, in addition to the development and maintenance costs, the state will in all likelihood also cover the private sector's profit expectations. This could lead to a situation where the price of a digital service is higher than what would be achievable in the conditions of open market competition. For the state, this represents an extra cost that could only be justified if there is no demand for the digital service in the private sector or if it fulfils a unique role that market forces cannot provide on their own.

Example

The early childhood education software Eliis, which is used by more than 700 educational institutions in Estonia, Latvia, Lithuania, Poland, Ukraine and Germany, is a good example of a universal and scalable digital service created and developed by the private sector. The digital service is universal in its nature, as it solves problems that are common to many countries and institutions – for example, diaries used in kindergartens, communication with parents, attendance management, reporting, etc. It is precisely this generalisability that makes it possible to offer the same software to multiple customer groups across national borders, thereby creating a wider user base and ensuring better cost-effectiveness. When comparing the cost of using the software and the amount of tax revenue the company generates for the state, it is clearly a digital service with a positive output.

Recommendations

1 **Assess whether the same digital service could be provided to the private sector as well.** The more standardised and universal the functionality of a digital service or product, the greater the opportunity to expand the customer base into the private sector. For example, if a digital service is meant for data exchange, security or identification, it may also have applications outside the public sector. A broader customer base would reduce the state's dependence on a single solution and increase the cost-effectiveness of digital services, as the participation of the private sector could help with sharing development costs.

2 **Analyse whether digital services can also be offered outside Estonia,** consult organisations representing entrepreneurs (e.g. Estonian Association of Information Technology and Telecommunications, Estonian Chamber of Commerce and Industry, Startup Estonia, sectoral associations/clusters) if necessary. If a digital service is scalable and, for example, complies with international standards, it may have the potential to find a market in other countries. This would mean that development costs could be shared between several customers, making the financing of the digital service more sustainable and less dependent on the state's budgetary decisions.

1.2 Assessment of market potential

Assessing the market potential is important when deciding on the development of a digital service, as it shows whether there are competitive service providers in the market that can offer high-quality solutions. If such providers are already operating and investing in innovation, the state's own development may be redundant or inhibit the market.

The market should be assessed both in Estonia and internationally, as many digital services are cross-border and scalable. If a similar solution already exists, it may make sense to take it into use or adapt it, rather than developing a new digital service from scratch. However, if there is no suitable solution on the market or if the private sector is unable to meet the public sector's requirements (e.g. security, data protection), development by the state may be justified. However, even in this case, it is preferable that the state should remain the owner and manager of the digital service, buying the development and management from the private sector. This supports the development of the local IT sector, provides flexibility and enables the use of private sector know-how. Such cooperation strengthens the functioning of the market, promotes knowledge circulation and provides companies with valuable references that are also useful when competing in the international market. The state's trust helps increase the trustworthiness of service providers and shows that they can create and manage digital solutions that are important to society.

1.2.1 Does a similar digital service already exist on the Estonian market?

Before developing a new digital service, it should first be assessed whether a solution with the same, a similar or sufficiently similar functionality already exists in the Estonian private sector and could be adapted to fit. If there is a digital service available on the market that meets the requirements of the public sector – e.g. in terms of quality, data security or accessibility – it may be considerably more reasonable and cost-effective to buy this solution than to start building a state-owned system from scratch. However, this requires a preparedness to adapt – the public sector needs to take into account that the digital products offered do not always have to correspond 100% to the desired specifications. The state must learn to use existing solutions where reasonable, adapting its processes and expectations where this is justified.

Example

The state itself has not developed digital payment systems to make transfers and move the money of citizens or companies. This task was left to the financial sector, which had more experience and competence.

Example

In many cases, the digital service to be provided is not related to the exercise of public authority or a unique public function. For example, various 'convenience services' (such as chatbots) or support activities such as document management services, whose solutions are widely used in the private sector, may not require special development by the state. For such digital services, the use of private sector solutions is not only sensible but also a responsible use of resources.

Recommendations

1 **Analyse the solutions available on the Estonian market a**nd their suitability or applicability to your needs. For this purpose, first do an online search to see if digital services or software solutions with similar functionality are already available – check company websites, lists of startups, read the news. If possible, contact service providers directly, ask for a demo, background and pricing information, etc.

2 **Consult organisations representing entrepreneurs** (e.g. Estonian Association of Information Technology and Telecommunications, Estonian Chamber of Commerce and Industry, other professional associations, Startup Estonia) to identify possible providers of a similar digital service on the market.

1.2.2 Which international solutions could be adapted to the Estonian context?

It is important to look at the market potential not only within Estonia, but also internationally, as digital services and products are often cross-border and scalable solutions. If a similar digital service is already provided in other countries or regions, it may be more practical to explore whether the existing solution could be used in Estonia, either through adaptation or licensing. Many technology companies are developing products for the global market, which means that the public sector of smaller countries, such as Estonia, can also order digital services from them. As is the case with the Estonian market, it must be kept in mind in the case of internationally available digital services that the introduction of a digital service from the private market requires a certain preparedness to adapt.

Example

All public authorities in Estonia use Microsoft products. In addition, the Moodle environment provided by the private sector is used as an e-learning environment, but the state itself plays the role of administrator and user support, thus adapting the solution to make it more suitable for users.

Recommendations

1 **Map the international solutions** that could be adapted to the Estonian context. See what other European countries are using, what open source solutions are used in other countries, what digital services are offered by private providers.

2 Consult with the authorities of other countries that offer similar services to their citizens. Many direct public services can be universal in their essence, i.e. the public authorities of other countries may already have the desired digital solutions.

1.2.3 Is the private sector interested in providing the digital service to the state? Is there a sustained demand for the digital service that would provide a stable cash flow for the private sector?

If there is no suitable digital service or functionality on the market at the moment, this does not automatically mean that the state should develop the solution itself. Before such a decision is taken, it should be thoroughly assessed whether the private sector has the interest and capacity to create the respective digital service. It is advisable to carry out a market analysis for this purpose – not just a formal request, but an active dialogue with potential service providers, for example through seminars, round table discussions, trade fair visits or direct contacts. In this way, information can be gathered on which sectors of the economy might be able to develop suitable solutions, which companies might be able to create the digital service, and whether and under what conditions they would be willing to invest in development.

It is important that the state as the first customer does not only focus on the existing market situation, but also assesses whether there could be a sustained demand for the digital service in the long term, which would create a stable cash flow for the company and a business interest to invest in the development of the digital solution. Only in this case can it be assumed that the digital service will remain sustainable also after the end of the state's development support or the order.

If the market analysis shows that the private sector does not have the interest or capacity to develop the necessary digital service – for example, because the solution initially appears to be very specific, risky or not commercially viable – the state may consider creating a digital service on its own initiative. In this case, it may be sensible to develop the solution in a way that allows it to be made available later, either free of charge as an open source code or on favourable terms. This way, it will be possible to avoid duplication and encourage the use of this digital service elsewhere, while ensuring that the public investment creates wider value.

Example

When the ID card was being developed, the state did not have an understanding of whether and how many private market providers might be interested in producing an ID card for the state. In order to address this issue, discussions were held in Estonia and a number of visits were made to foreign companies to clarify what was wanted and give reassurance about the readiness to buy the service. The chosen approach was successful – Swiss company Trüb AG submitted a tender in the procurement for ID card production. (see the story of Estonia's digital identity: public-private partnership)

Recommendations

1 In order to better understand the potential of the market, it is wise to carry out in-depth market research. For this, we recommend:

- Carry out market research in all market segments where the capacity to provide a solution to the problem could be presumed.
- Document the market research, at least in a format that can be reproduced in writing. When preparing the documents of the market research, keep in mind that:
  a. this cannot be treated as a base document for public procurement or a call for competition (so as not to create unnecessary ambiguity if a recipient of the request makes a tender as a result of this); and
  b. neither the submission of, nor responding to, a request for information is legally binding on either party.
- Take this input into account when making the next decisions, e.g. when preparing procurement documents. If, for example, the market research shows that submitting a tender might be unreasonably expensive, consider the possibility of partial or full compensation of the costs involved.
  a. More specifically, the Public Procurement Act allows the contracting authority to compensate the costs incurred by tenderers in the framework of different procedures. For example, in the case of a competitive dialogue, the contracting auhority may award prizes to tenderers or pay a participation fee to compensate the costs incurred in developing the solutions proposed during the dialogue, the amount of which may vary according to the suitability of the solution proposed in light of the established conditions. Participation fees and compensation for costs shall be included in the cost of the planned procurement.

2 Assess whether there is a sustained demand for the digital service that would provide a stable cash flow for the private sector in the provision of the service. If there is only temporary or low demand for the digital service, the private sector may find it difficult to achieve profitability and motivate investment. Sustained demand gives the reassurance that the private sector can provide the solution sustainably and cover the development and maintenance costs. If the private sector lacks certainty about the long-term viability of a digital service, this can hold back investment and innovation.

- It is worth considering whether the digital service may be needed by several public authorities. If yes, and if each of them individually is not a large enough contracting authority to make the provision of the digital service in the market profitable for the private company, consider centralised or joint procurement. In this context, marketplace solutions may be considered, where a digital service is procured in a simplified way using the framework contract model or a dynamic procurement system.

1.2.4 If there is no such digital service or interest today, could the state be the first customer and thus create a market?

In certain cases, a digital service may have strong market potential, but there may not yet be a corresponding private sector solution on the market. In this case, the state can take an important step as the first customer by commissioning or developing the necessary solution itself, which opens the way for the emergence of new market-based digital services.

'The state as the first customer' can provide a supportive environment where innovative companies – especially startups and small and medium-sized enterprises (SMEs) – can test and develop their solutions securely, with the actual user. This will help overcome the situation where companies are reluctant to invest in new solutions until there is a solid demand, and customers are reluctant to use a digital solution until it has proven itself in the market.

However, if it turns out that the private sector does not have the interest or capacity to develop the necessary digital service, the state can create the solution itself first. In this case, the state could strategically decide that the software will be made available as an open source or transferred on favourable terms at a later stage to support wider use and avoid duplication. This way, the state can meet a societal need while maintaining flexibility for the future, should the interest of the private sector grow.

Recommendations

1 Carry out market consultations to identify market potential.

2 Consult organisations representing entrepreneurs (e.g. Estonian Association of Information Technology and Telecommunications, Estonian Chamber of Commerce and Industry, Startup Estonia, sectoral associations/clusters) and use their contact network to find out about market potential.

3 When procuring an innovative digital service, opt for types of procedure that support the procurement of innovative solutions. For example, organise the procedure as a competitive dialogue, a competitive procedure with negotiation or an innovation partnership. An innovation partnership is a suitable type of procedure where the need to develop and subsequently acquire an innovative digital service cannot be met by solutions already available on the market. An innovation partnership is a specific procedure used to create a long-term partnership for the development and subsequent acquisition of a completely new solution, provided that such an innovative digital service can be provided with the agreed quality and price without the need for a separate procurement procedure foracquisition.

4 If the digital service is owned by the state or if the state decides to develop it itself first in the case of a market failure, plan the decision point and the actions to transfer or grant the right to use the state-owned intellectual property (digital solution).

- If the private market is ready to take over the provision of the digital service and this is economically reasonable, it must be considered whether the successful provision of the digital service requires allowing the private sector partner to use the intellectual property belonging to the state or transferring it to the partner.
- In order to find a private market operator and to allow just one exclusively selected company to use the intellectual property belonging to the state/transfer it to the company, it would be worth using the procedures that allow the state to take advantage of the competition most efficiently, e.g. by organising an auction. The procedures laid down in the State Assets Act must thereby be taken into account.
- It is also possible to grant the right to provide the digital service and the intellectual property necessary for the provision of the digital service on the basis of a concession contract. A concession contract for services is by its nature a public contract where the fee for the provision or organisation of a digital service consists either solely of the right to provide or organise the digital service or that right with a monetary payment and the business risk associated with the demand or supply is transferred to the concessionaire. The conclusion of a digital service concession contract is preceded by a procurement procedure.
- In a situation where the state has made the source code of software belonging to the state available to the public free of charge in the manner provided for in the State Assets Act, there is no need to organise any special procedures, but the right to use the software can be granted to a company on the basis of a licence agreement.

1.2.5 What mitigating measures can be taken to avoid a vendor lock-in?

Vendor lock-in may occur if there is only one or very few providers in the market, which can lead to price increases, lack of innovation and poor quality of the digital service. The public sector must assess whether there is sufficient competition in the private sector to ensure that the digital service remains cost-effective and innovative, and its quality does not deteriorate.

It there is only one provider on the market at the moment, this does not automatically mean that the involvement of the private sector in the provision of the digital service is excluded. Rather, in such a case, it is necessary to be prepared for possible unexpected occurrences (e.g. the provider of the digital service stops trading), and to create favourable conditions for competition by involving the private sector.

Example

The Estonian Information System Authority recommends using the MIT licence[3] in software development, and the increasing value in using the EUPL licence[4] is seen in Europe. Both licences give the state and the company the right to develop the solution further, sell it if necessary, and provide support to other users. This approach allows the state, as the first customer, to support the launch of a new digital service or product in a way that creates opportunities for the company to further develop the solution, attract new customers and grow the scope of its business.

Recommendations

1 When procuring solutions, carefully consider the terms and conditions of using the intellectual property linked to the solution. For example, it is worth giving the contracting authority the broadest possible right of use (licence) that allows it to develop the solution further, modify it, give it to subsequent tenderers, etc. It must be kept in mind that the state also has a right to the intellectual property of the final solution and the associated licence if the solution has been created with input from the state's employees or experts.

2 Consider whether it is possible to set up or procure a solution in a way that would result in the cooperation of several tenderers (consortia), and also check that the eligibility and qualification conditions of the procurement encourage the participation of SMEs and the emergence of consortia. Assess whether the turnover requirements imposed allow smaller companies to participate, whether the experience requirements favour companies that have been on the market longer, etc.

3 In the case of the risk of just one vendor, think through the duration, terms and conditions of the contract to be awarded. The longer the duration of a contract with a single vendor, the greater the risk that the market will lock in favour of one vendor for a longer period. Other vendors in the market must be regularly given the opportunity to compete in the event of the risk of a single vendor. This can be done by making the data volumes, user satisfaction and associated public costs of the digital service cases transparent, giving the market the opportunity to respond and offer alternatives.

3 https://en.wikipedia.org/wiki/MIT_License
4 https://en.wikipedia.org/wiki/European_Union_Public_Licence

1.3 Risk assessment

An analysis of the potential risks is crucial in assessing the possibility of cooperation with the private sector. Outsourcing the digital service or its provision by the private sector can offer efficiency and innovation advantages, but at the same time it can create challenges in terms of data protection, consistency, availability and independence. It is therefore important to carry out a thorough risk analysis to ensure the quality, reliability and security of the digital service. The control question “What are the main risks that can occur when delegating or outsourcing a digital service?” helps identify and anticipate potential risks, supporting an informed and well-considered decision-making process.

Often, various concerns – such as data protection, security, or vendor lock-in – are cited as a reason for the state to develop its own digital service, but these may not be real obstacles. In most cases, these are manageable risks where suitable contractual, technical or organisational solutions can be found, which will bring the impact and probability of the risk down to an acceptable level. Instead of fearing risks, they should be acknowledged, assessed and managed – this is how flexibility can be maintained and the benefits of private sector solutions can be used.

1.3.1 Which security requirements must be followed when providing the digital service?

Confidentiality issues may be important in the context of the exercise of public authority and the digital service. For example, information disclosed in the course of the provision of a digital service may be protected by access restrictions within the meaning of the Public Information Act or declared confidential, including classified as a state secret. However, the confidentiality of information does not mean that such information cannot be disclosed to a private sector partner under any circumstances, i.e. confidentiality of information does not rule out the involvement of external partners. If involvement in the provision of a digital service requires the establishment of special rules to protect the confidentiality of information, including the verification of the trustworthiness of the persons involved, it is possible for the state to establish such requirements either through the conditions used in the procurement procedure or in a contract. It is important to keep in mind that when external partners are involved, their trustworthiness can also be verified and guaranteed with the same measures used to verify and guarantee the trustworthiness of the state's officials.

Example

The border protection project KILP, which is managed by the Information Technology and Development Centre of the Ministry of Social Affairs (SMIT), involved specialists from several well-known Estonian IT companies in the development work, who were subjected to background checks similar to SMIT's own employees, and security requirements were established to ensure the reliability of their work. Although most of the work was carried out in the offices of SMIT, in some cases the development was also carried out off-site – in case like this, installations and access to sensitive environments were always carried out on the premises of SMIT. In practice, SMIT treated these outsourced experts as part of its team. Technically, it would have been possible to outsource the development of all the sub-components of the digital service and order a readymade solution based on data models and specifications. The project also involved companies whose specialisation in hardware and software development offered the state critical expertise that would not have been reasonable for the state to have itself. Related security risks were systematically mitigated through background checks and contractual obligations, ensuring that the work was reliable and could be inspected.

Recommendations

1 Clarify what security requirements need to be implemented to ensure the confidentiality of the information and the trustworthiness of the persons involved. Requirements should be established if your own officials/employees are expected to undergo background checks or follow specific confidentiality requirements in this area.

2 If the initial analysis showed that certain security requirements must be imposed on the service provider or on cooperation with the private sector, describe them in more detail and decide how you can enforce them. Possible options:

- **Requirement for security clearance to state secrets**
  a. Determine the level of classification of state secrets.
  b. Develop ways for requiring private sector partners to comply with this requirement.
  c. For example, in a procurement procedure, one of the criteria could be the requirement to have facility security clearance by the time the contract is awarded. As the application for security clearance takes time (about 6 months), this should be taken into account in the procurement procedure.
  d. If you have identified that a private company needs to process state secrets on its own premises in order to carry out the work, ask the private sector partner to apply for facility security clearance. If an employee of the company carries out all the work on the premises of the contracting authority, it is sufficient if the employee has personnel security clearance. Every employee who will be processing state secrets must apply for personnel security clearance separately.
- **Background check**
  a. If you have established that a security clearance is not required, but the information is nevertheless particularly sensitive, you can set requirements for the background of the persons processing the information (e.g. criminal record, existence of references, etc.).
  b. In a procurement procedure, it is possible to request that the persons involved in the performance of the contract and in the development of the digital service offer/solution undergo the background check required by the contracting authority. In such a case, the legal basis for undergoing a security check is usually the person's consent and/or the basis for performance of the contract.
- **Non-disclosure agreement (NDA)**
  a. If sensitive information is disclosed within the scope of a procurement, the contracting authority may require the conclusion of a non-disclosure agreement to protect the information.
  b. Confidentiality clauses may be included in the contract to be awarded, but it is also possible to require the conclusion of a non-disclosure agreement before the more substantive publication of the terms and conditions of the procurement. For example, the contracting authority can publish part of the technical specifications in the public view in the procurement procedure, and the rest of the documents/technical specifications can be accessed by the tenderer if it agrees to undergo, for example, a background check and/or sign an NDA.
  c. It is reasonable to ensure confidentiality by means of a contractual penalty, which would allow the company to recover damages more easily in the event of a breach of confidentiality.

1.3.2 What quality requirements must be followed when providing the digital service?

The opinion that digital services developed in the public sector are of higher quality than those of the private sector is generally not justified. Companies in the private sector specialise in software development and operate in constant competition, which forces them to provide user-friendly, secure and technically up-to-date solutions. They have direct contact with the needs of diverse customers, the ability to respond quickly to changes and the motivation to deliver scalable and innovative digital services. Although public authorities are bound by public interest in their objectives, this does not automatically make them better developers – they often lack the specific skills or resources necessary for this. Quality depends primarily on the organisation of the development process, substantive cooperation and clear requirements, and not on whether the developer works in the public or private sector. If the same quality standards apply to the private sector, there is no reason to assume that a solution developed by the state would be better – on the contrary, well-managed cooperation with the private sector often allows for faster and more scalable results.

Recommendations

1 Think about the quality requirements or standards that the digital service provider/developer has to apply.

2 Are the required standards specific to the public sector, i.e. they cannot be implemented by private sector companies?

3 Check whether the current legal framework gives the state the option to supervise the provision and quality of the digital service and assess whether such inspections are necessary.

- If the present regulation is not sufficient, prepare amendments and enforce them.
- Supervision can also be described in the decision to delegate a digital service (contracts), as well as in the public contract if it is decided to outsource a digital service or its development.
- When establishing new additional requirements, consider thoroughly whether they are practical. Supervision is a cost to both the state as the supervisor and the private sector (as the supervised), and incurring this cost should outweigh any potential harm that may emerge.

1.3.3 Does the provision of the digital service have to comply with security standards that the private sector cannot meet?

It is not reasonable to assume that digital services commissioned from the private sector are less secure than solutions developed by the state. The level of security does not depend on who develops the digital solution, but on the requirements and controls that are established for the development. Developments made by the state are not automatically more secure – the same risks (such as data leakage or system failure) exist in both cases. Developers in the private sector often follow internationally recognised practices and standards, and if the state defines clear security requirements for digital services, it is possible to ensure the same or even a higher level of security than in the case of nationally developed solutions.

Example

The state can ensure the protection of personal data in the case of digital services ordered from the private sector if the contract and the terms of the service clearly state the requirement to comply with the General Data Protection Regulation (GDPR). The service provider can also be required to implement security measures for information systems in accordance with the international ISO/IEC 27001 standard.

Recommendations

1 Decide whether the provider of the digital service (private sector company) needs to undergo a security audit. If yes, establish it as a requirement.

2 Can the state supervise the provision of the digital service to monitor that security is being ensured if necessary? (see also the recommendations on supervision in the previous chapter)

1.3.4 What technical requirements should be imposed on the digital service?

When a digital service is provided by the private sector, users expect the same quality as from a digital service provided by a public authority. Therefore, a digital service of the private sector must also comply with the same principles and requirements as if it were a solution developed and managed by the state.

The architects of public services have established the state's interoperability framework[5] , which defines the general principles for the development and operation of digital services. The cross-functional[6] requirements that apply to all services of the digital state regardless of the service provider are also part of this framework. These requirements cover the quality of the digital service, information security, technical interoperability and other important underlying principles. It is a comprehensive set of requirements, for which it is generally not necessary to set additional general requirements – they cover the whole necessary baseline.

The expectations of users must also be taken into account in terms of the availability of digital services. According to the analysis of the Estonian Information System Authority[7] , 68% of users prefer state services to be accessible through the state portal eesti.ee. Therefore, the suitability for integration with the state portal and the state's SSO solution must also be assessed in the case of a digital service from the private sector. Micro-frontend solutions are increasingly used for this, as they make it possible to provide a digital service directly in the state portal environment, while maintaining a consistent and seamless experience for the user.

Example

In addition to general architectural and security requirements, specific functional and non-functional requirements may apply in different areas. For example, e-health solutions must comply with sectoral data standards and other established requirements. In the case of such specific conditions, it is not only important that they are followed, but that their relevance is regularly assessed to avoid the preservation of outdated or disproportionately burdensome requirements.

Recommendations

1 When procurement is organised and contracts are awarded, the focus should primarily be on a clear description of business needs and expectations, rather than listing overly detailed functionalities. Over-specification can limit the flexibility of the development of the digital service or product and be an obstacle to making necessary changes, as they may be in conflict with the procurement documents or the contract.

2 At the same time, it is important that the procurement terms and contracts clearly stipulate the requirement for compliance with the interoperability framework of the digital state and, where applicable, cross-functional requirements which ensure that the digital service is compatible with the state's overall technical and security requirements:

- Take into account the use of the consent service, eID, data tracker and other subservices expected by the state, according to the needs and functionalities of the digital service.
- When databases and data services are issued, expectations must also be set for the national data exchange platform X-road if sensitive data and requirements related to disclosure are involved.

3 Also, think about the specific sectoral requirements that apply and set these as conditions for the provision of the digital service in the procurement and contract.

4 Don't forget supervision when setting requirements. Carry out a pre-launch review of compliance during the development stage of the digital service and periodic supervision during the provision of the digital service.

5 https://digiriik.eesti.ee/koostoimeraamistik
6 https://digiriik.eesti.ee/koostoimeraamistik/5-tehniline-koostoime-ja-rakendused
7 https://www.ria.ee/sites/default/files/documents/2022-11/Riigiportaali-eesti.ee-rahuloluanaluusi-koondaruanne-2020.pdf

1.3.5 Can the state impose requirements for the sustainability of the digital service?

The sustainability of digital services is critical for the public sector, as many services perform socially important functions and their disruption or the deterioration of their quality could directly affect people's rights, security or trust in the state. The provision of a digital service does not end with its development or introduction – it is important to ensure that the service works in the long term, is technically up-to-date, secure and accessible, and can adapt to changing needs and environments. This is particularly important when the service is provided by the private sector: the state must have reassurance that the service will not be unexpectedly interrupted and that mechanisms are in place to take it over, develop or replace it. Sustainability is not only a technical issue, but also involves contractual, organisational and strategic decisions that affect the performance of the service throughout its lifecycle.

Example

The Ministry of Education and Research used the option of a notarial deposit in the case of the international student admissions system (a solution created by DreamApply OÜ). Notarial deposit allows the source code of the software created for the digital service to be deposited with a notary. This depositing model makes it possible to preserve software that is important to the customer, while mitigating the risk of the developer's insolvency leading to the end of the provision of the digital service (see DreamApply).

Recommendations

1 **Consider using more flexible forms of cooperation,** such as concession contracts, which give the service provider greater freedom to manage its digital service, but allow the state to set clear requirements for the continuity of the digital service.

2 **Assess the conditions** under which the digital service may be temporarily and permanently interrupted.
- Temporary interruptions should be described in service level agreements (SLAs), specifying, for example, response times, permitted duration of interruptions and penalty mechanisms.
- Regulate the end of the service in the service contract – set long notice periods, a mandatory transfer period and a transition plan.

3 **If necessary, arrange for the digital code to be deposited with a notary** so that the state can get the source code and continue the service in a crisis.

4 **Prefer open source solutions** where possible and reasonable, to reduce dependency on a particular vendor and to encourage subsequent development by other parties.

5 **Prepare a contingency plan in the event of a digital service disruption,** describing the actions to be taken, the responsible parties, contingency plans and the resources needed. Include the possibility of a rapid takeover of the service by the state or a third party.

6 **Ensure data independence and availability.** If necessary, stipulate in the contract that all data collected during the service will belong to the state and must be available at any time in a standard format via X-road.

1.3.6 Are there any strategic activities that the state as the policy-maker and service owner could no longer carry out if the digital components of the service were (partly) owned by the private sector?

The role of the service owner in a strategic context is to define the objectives, directions and development plans of the service, ensuring that the service as a whole supports the strategic goals of the organisation or the state. This includes ensuring the quality, availability and long-term sustainability of the service. The service owner decides whose needs the service meets, the value it creates and how the service as a whole is developed and updated. In the context of the state, ownership of a service also means representing public interests and that the service achieves socially important objectives.

This guide does not focus on the ownership of the service as a whole, but primarily on the ownership and provision of the digital service, i.e. the digital component of the service. A digital service is not an independent type of service, but a way of delivering part of the content or process to the user. Most public services are hybrids and contain both digital and non-digital components, such as human labour, physical presence or administrative operations. Therefore, the ownership and organisation of both the service as a whole and its digital component can be decided separately.

In Estonia, the organisation of digital services is often structured in such a way that the service owner is located in a ministry, authority or inspectorate, while the product owner is based in the state's IT centre. Decisions on the development and provision of digital services must be taken in cooperation between the two roles, as they clearly have different areas of responsibility. For example, only the service owner can initiate legal amendments, and it is the owner's responsibility to define the strategic direction of the service and ensure that public interest is represented. The product owner, on the other hand, must ensure that the digital service is technically feasible, of high quality, secure and compatible with the state's interoperability framework. Deciding on the provision of a digital service is the responsibility of the policymaker, i.e. the service owner; the role of the IT centre, as the product owner, is to support this decision with the necessary technical support and expertise.

In summary, decisions on the ownership and management of digital services must be taken in cooperation with the different stakeholders, in line with the state's strategic need to influence the provision of digital services. Where the state has a major role in shaping a digital service, it may be practical to own the digital service and retain more substantive control over it. However, if strategic intervention is not necessary and the private sector has the capacity to ensure the quality and continuity of the digital service, the state can focus on channelling the digital service through regulation and supervision.

Recommendations

1 Consider whether the state needs to shape the vision and business direction of the service or digital service. What is the difference between these two views?

2 What are the potential strategic risks associated with the provision of the digital service by the private sector?

- Carry out a thorough risk assessment, describing the risks, their likelihood and potential impact.
- Develop mitigation measures to be implemented if risks materialise
- Appoint the persons responsible for risks.
- Determine the regularity at which the risks and their materialisation and impact are reviewed again.
- Decide whether the described mitigation measures bring the risks to tolerable levels. If not, decide whether it is possible to involve the private sector in the provision of the digital service.

Annex 1

Examples

The story of Estonia's digital identity: public-private partnership

The journey of Estonia's digital identity officially started in 2000 with the adoption of the Digital Signatures Act. It created the legal basis for the use of electronic signatures and marked an important step in the development of the e-state. Before that, the Ministry of the Interior and the former Citizenship and Migration Board (now the Police and Border Guard Board) had been preparing the ID card concept for several years, studying international standards and creating a development plan. This was more than just the preparation of a new document, it was part of a bigger vision – to give people a digital identity that could be used for both public and private sector services.

Limited resources force innovation

When launching the ID card service, the state was faced with a situation where its own resources were insufficient for covering all the initial investments – there were no funds for the creation of the technology needed for personalisation, certification and card production. However, the private sector could raise investment money, take out development loans and therefore move faster. This is what led to the decision to outsource ID card services. As the Estonian market is small and its potential was unknown, then simply hoping that service providers would respond to a procurement was not an option. Officials travelled around Europe talking about our plans and trying to convince potential tenderers that Estonia was ready to buy the service if someone could develop it. The tactic proved successful – the Swiss company Trüb AG was chosen to produce the ID card in 2000, and the certification service was offered by two tenderers who did not have a ready-made service, but were willing to create one. The win-ner was Sertifitseerimiskeskus AS (now SK ID Solutions AS).

Need creates new services

A number of e-services, such as e-School and the e-Land Register, started to develop rapidly alongside the introduction of the ID card. However, it turned out that the ID card was not suitable for all situations. For example, it could not be used abroad or in computers in Estonia where it was not possible to install the necessary ID card software.

This led to a new need – a mobile identification tool. The idea for Mobile-ID came from the Vaata Maailma Foundation and EMT (now Telia) launched the service in 2007. At first, it was only available to EMT customers, but by the following year other mobile operators joined when they realised that without Mobile-ID, they would lose valuable customers.

The innovations were accompanied by regulation, so an amendment was made to the Identity Documents Act in 2009 that officially recognised digital identity – the document type 'digital identity card' was added. It was a landmark innovation, because it allowed people to also identify themselves securely and reliably in a fully digital environment, without the need for a physical document. The amendment made a year later allowed digital ID to exist 'in the form of Mobile-ID', making Mobile-ID a nationally accepted means of authentication.

When the market does not meet expectations

A difficult situation emerged in the early 2020s: the law required that SIM card-based authentication services should remain in use, but a suitable offer could not be found in the market. SK ID Solutions, which had been providing the service until then, shifted its focus to the substantive development of Mobile-ID in a more cost-effective way internationally (SK provides the service on the EE and LT markets) and was not interested in continuing the service specifically designed for the Estonian state. As a solution, the state entered into a concession contract with SK ID Solutions, which gave the service provider more freedom to manage its service, but at the same time set out clear requirements for service continuity and quality (e.g. 1-year notice period for termination of service, requirements for identity checks, possibility to revoke a national document, etc.). The service provider was given a clear framework to follow and the state was able to ensure continuity of service. The Identity Documents Act was also updated in 2022 to make it possible to introduce solutions based on the eSIM technology, which eliminated the state's dependence on the Mobile-ID service.

The story of Estonia's digital identity: public-private partnership

Lessons from this example

- **It is important to understand how critical service continuity is.** If there must be no interruptions in the service, the state must have a clear mechanism in place to ensure its availability – whether that's ensuring continuity through contractual obligations (e.g. notice of termination of service must be given a long time in advance), depositing the code with a notary, contractual relationships with a number of physically and logistically independent providers, or readiness to take over the service itself.

- **When a new service is created, it is important to assess whether the state has the resources to invest in the creation of the digital service.** If the budget is limited, finding a private sector partner may be the only practical way forward.

- **In Estonia, not every service has to be built from scratch. There are already many working digital solutions on the market that can be adapted or introduced according to the needs of Estonia.** Estonia is too small a market for many services being created in a unique way to make economic sense, so strategic choices should be made to adapt to the services on the market. We are learning to use universal tools such as Microsoft 365 according to these rules; we've also realised that Zoom or Teams as communication channels are suitable solutions for the public sector. Other digital services and products can be treated in the same way.

- **When procuring services, functionalities should be described in more general terms.** The state should say what is needed and request tenders, not describe how the service should work in detail in a procurement or public contract. This leaves room for the service provider to improve and develop its solutions according to user feedback and market changes. More attention should be given to non-functional requirements such as availability, reliability and security.

- **The role of the state in digital services is not to be a developer, but the creator of the environment.** Once the rules, requirements and supervision mechanisms are in place (which provide a certain guarantee of service quality), all parties can play their role clearly and effectively. This is how reliable and sustainable digital services and cooperation are created.

DreamApply

The launch of the common admissions system for foreign students of Estonian universities dates back to 2008, when the development of the DreamApply student admission service started. The company struggled to find its first clients, but in 2011, the Stockholm School of Economics in Riga became its first client. At first, there were no plans to offer the service on the Estonian market, but in the same year the company was contacted by the Estonian Information Technology Foundation (EITSA), which was planning to set up an admission system for foreign students at the request of a consortium of Estonian universities. The original plan was to take the best features of existing private sector solutions and build an entirely new information system based on these, with further management by the state. However, after the presentation of the DreamApply service, it was agreed that the private sector solution was already suitable and that problems of which the state had not been aware had been considered when the solution was created. The decision also made economic sense, which is why the state decided to outsource the digital service to the private sector.

Building trust and managing risk

At the time, there was some mutual mistrust and uncertainty between the company and the state, as the EITSA team was unsure whether the small company would be able to provide the digital service in the long term. Therefore, a notarial deposit agreement was concluded from the outset – the source code of the company's software was handed over to a notary for the management of the customer's risks and, if necessary, for the continuation of the offer of the digital service by the state, which at that point took place in the notary's office with a CD. Although this approach initially seemed alien to the private sector, from the viewpoint of the state and the universities, it was a necessary step to mitigate potential risks and ensure continuity of the digital service. At the same time, a convincing argument for both the EITSA and the universities was that the digital service could be used quickly and was cheaper than building and maintaining the system themselves.

Partnership dynamics and communication lessons

In 2012 and 2013, the digital service and cooperation worked successfully and smoothly, eliminating the need for regularly updated audits as the company gained new clients and confidence in sustainability increased. Changes in the customer's organisation (the EITSA was merged with the Information Technology Foundation for Education) and in the project managers made the relationship between the company and the state more formal and communication became weaker. From the company's perspective, the state no longer had an expert who understood digital services and the mechanisms of private sector digital services, and could engage in meaningful dialogue with the service provider. The pricing model of the digital services therefore became a major challenge in 2014.

The private sector offered digital services at a minimum price, but the state still considered it expensive, mainly because the pricing structure was unclear from the state's perspective. This led to tense negotiations and the need for more transparency in pricing. The company also suggested holding regular meetings, which would have helped strengthen cooperation between the parties and reduce communication problems. Despite the change of the customer and the project managers of the state, the digital service has worked well to date and has been approved by both Estonian and foreign universities. At the same time, tensions in price negotiations between the state and the private sector have continued to recur, pointing to the need for a pricing framework that is more precise and easier to understand.

DreamApply has grown into an international company whose services is being used by 300 universities worldwide in 2025. The company's turnover has reached almost €3 million and it employs more than 20 people in Estonia and abroad. A common admissions system developed by the state would be expensive for the state as a digital service, but as an international exporting company, it becomes a tax revenue generating enterprise.

Lessons from this example

- **Depositing the digital service code should be a normative and culturally accepted practice** in the procurement of digital services in the Estonian public sector to ensure service continuity and mitigate risks. However, depositing should be discontinued as soon as it is no longer necessary.
- **Transparent and understandable pricing is essential** in order to avoid tense negotiations and to ensure that the parties understand each other's positions. The state needs people who can communicate with the private sector, understand the specifics of digital services and manage relationships strategically and for the long term.
- **The state should identify competitors to avoid vendor lock-in and ensure continuity and availability of digital services.**
- **However, at the very most, the state must be prepared to set up the digital service itself.**

Food cards – how the private sector provides services more efficiently than the public sector

Before the transfer to food cards, the Ministry of Social Affairs organised food aid purchased by the state in the form of food aid packs, which were distributed to people in need four times a year. In order to procure food products, the Ministry of Social Affairs organised public procurement through which a wholesale company was found as a partner. The Ministry of Social Affairs and the Food Bank with volunteers and social workers from local authorities took part in the distribution of the packs. However, the contents of the food packs did not meet people's needs and they had to queue to get the packs and carry the heavy bags home. In the budget of €2.5 million in 2022, administrative costs accounted for ca €200,000, i.e. 7–8% of the total budget allocated to purchased food aid.

Solution

An aid card was developed and €30 is transferred onto the card per recipient every quarter. They can use them to buy food from the stores of the procurement winner all over Estonia, and also from the e-shop. Using a food card gives people in need the freedom to choose the food and essentials they want. The food card cannot be used to buy alcohol, tobacco products, lottery tickets or gift cards.

Preparations

Planning the transfer from food packs purchased by the state to food cards took years. The recipients of food aid, representatives of shops and local authorities were interviewed. Best practices from around the world were mapped. The costs of the old system and of the possible new system to be created were assessed.

IT developments were also prepared in the database so that the whole system to be created would be paperless and the chances of human errors occurring would be minimal. The original plan to use the national STAR information system for data exchange was replaced by a more flexible but equally secure cloud solution.

The most difficult part was generating interest among potential parties. Round tables were organised with shop representatives. One of the fears they highlighted was the paperwork involved in dealing with the state. Several different lawyers helped prepare the public procurement to solve all the data protection and other issues. An open procedure over the international threshold was chosen as the type of procurement and the successful tenderer was awarded compensation for adapting its systems.

All stores were invited to participate in the public procurement through the Estonian Traders Association. The first procurement resulted in one tender. Corrections were made in the second procurement according to feedback and the result was 2 tenderers. The winner of the procurement developed the food card platform itself in-house to meet all the requirements set in the procurement (exclusions, analytical capabilities, etc.).

Results

The food cards project was launched in 2023 and has been a success so far. A nationwide system of food cards is a first in Europe and has never been implemented on such a large scale before. It's an example for other countries on how to help the most vulnerable members of society in a flexible and dignified way.

1. For the person in need:
   - Using a food card gives people in need the freedom to choose the food and essentials they want.
2. For the company:
   - The winning tenderer developed a home delivery service for customers in a certain region, which helped them expand the service for commercial use and to also offer the service to other customers, not just people in need.
   - The monthly fixed costs of the food card do not depend on the number of aid recipients or the financial volume of food aid – a monthly fee is paid to the procurement partner.
   - The winner of the procurement was given a new market opportunity and a business model that can also be used in other Baltic States.
3. For the state and local authorities:
   - This freed up a lot of time for social workers of local authorities, which they can now use for counselling instead of packing food.
   - Administrative expenses decreased by ca 1.5%.
   - Only the food and convenience goods bought by the person in need are paid for.

Lessons from this example

- Nobody likes change – talk to people. Local authorities had to be persuaded that their lives would get easier. The winning tenderer convinced its management that there was a business opportunity in this.
- Don't be discouraged by doubters who may think that the desire to work with the private sector is motivated by personal gain.
- The procurement and the system are structured in such a manner that when the procurement period ends, other tenderers will be able to submit tenders, as compensation is foreseen for the adaptation of systems.

Bürokratt

Bürokratt is a way for the user to access public direct services and information services through virtual assistants with voice communication. The basic platform of Bürokratt is open source and available for anyone interested. Various services that are being introduced in different public authorities will in turn be interfaced with the basic platform.

The analysed digital service has not yet been fully developed. Below, we describe the ways in which the state could implement this digital service, taking into account the existing technical capacity, organisational side and market interest. The RIA is currently engaged in the implementation of digital services – both through its staff and by outsourcing services. In order to make the solution work more smoothly and flexibly, it would be sensible and necessary to involve private sector partners.

Implementation of the desired solution

On a broader scale, there are 2 alternatives: organising a concession procurement or organising a classic framework procurement.

If the market analysis or consultation shows that the private sector is willing to develop and provide the solution independently and the state does not want to cover the development costs itself, a concession contract could be considered. This means that the development and provision of the service will be placed entirely in the hands of the private sector. At the same time, the state can enter into contracts that make it possible to use the intellectual property that belongs to the state. Such a solution is particularly suitable when there are entrepreneurs in the market who see business potential and are willing to implement it at their own risk.

However, if the state is willing to cover the development costs and outsource the digital service, this requires the organisation of a procurement. The best way to implement this initiative would be a public procurement, the objective of which is to implement this initiative would be a public procurement, the objective of which is to award a framework contract. It would allow the state to outsource digital services from multiple providers, taking advantage of competition in the market. The customer could be either a certain single public authority or several authorities together, depending on how the project funding is organised (i.e. whether the money is managed by one or several contracting authorities).

In the case of a planned public procurement, the most important thing would be to think carefully about the terms and conditions of the procurement, the basis for the award of the framework contract and the terms and conditions of subsequent contracts. The technical specifications of the procurement should describe the type of digital services that are to be developed – in other words, the contracting authority should have at least a general idea of the functions that the solution should perform.

In addition, procurement should take into account how the partners who will be implementing the digital services are selected. This means rethinking the terms and conditions of the public contracts to be awarded on the basis of the framework contract. Past performance can be assessed when selecting partners – for example, how quickly and to what extent they have delivered services in the past. Payments can also be linked to whether the services are delivered on time and in the agreed volume.

If cooperation with several partners at the same time is sought and the target number of the services is known, it is possible to award a framework contract to several parties so that all the terms and conditions of the public contracts and the award procedure have already been agreed upon in advance in the framework contract. For example, the division of labour between partners can be based on a formula that takes into account their past performance. Also, if contracts are awarded later through the reopening of a competition, the quality and speed of their previous work can be taken into account when selecting the successful tenderers.

Annex 2

Myths and reality

Often, different parties have already developed attitudes or preconceptions before working with the private sector. These may be based on personal past experiences, cases shared by colleagues or isolated examples reported in the public. Such attitudes do not necessarily reflect objective reality, but refer to risks that can be consciously managed. When well-thought-out risk management measures are applied, the likelihood and impact of possible problems can be significantly reduced.

The following is a selection of the most common objections to cooperation with the private sector in the provision of digital services. All these topics are covered in more detail in the guide.

1 Services provided by the private sector are more expensive than providing the service ourselves.

This opinion is often based on the fact that we don't know how to compare the price of a digital service in the public and private sectors. In the public sector, cost models are not based on digital services, so there is no accurate over-view of the costs incurred by the state in providing digital services. The private sector, on the other hand, prices its services thoroughly, covering the day-to-day running costs, management costs, as well as profit expectations, etc. with the selling price of the service. The reality is that the majority of digital service costs are the same for the private and public sectors, but if a private sector provider has more than one customer, the total cost per customer is lower. See also 1.1.1 and 1.1.3.

2 When the state commissions innovation, it always has to pay for it in full, while the private sector makes a profit out of it later.

It is widely thought that if the state wants an innovative solution, it has to pay for its development in full, while the private sector can later resell the digital service it creates to others. In reality, however, outsourcing digital services may be the right solution for the state, especially if making a large initial investment is not possible, but the private sector sees a wider market potential in the solution. If the state can reassure the developer that it will become a user of the digital service – for example, as a clearly defined and stable customer – the private sector can take on a large part of the development costs itself. This "state as the first customer" approach allows innovative solutions to be brought to the market without all of the financial and development burden falling on the public sector. It is also often overlooked that a first order made by the state can be an important growth opportunity for a company. This will help it establish itself in the market, expand into foreign markets and become a major employer and taxpayer. This way, the state's initial investment in digital services can be recouped in the long term through tax revenues, export capacity and a stronger business environment. See Chapters 1.1.4 and 1.2.4.

3 It is dangerous to cooperate with the private sector when dealing with security or other sensitive information.

In reality, the same security and safety requirements can and should be imposed on private sector service providers as apply to the authority's own employees. See 1.3.1 and 1.3.3.

4 My service is a core service of the state, so we have to provide it ourselves.

This guide does not focus on ownership of a service as a whole, but primarily on the ownership and provision of a digital service, i.e. the digital component of a service. A digital service is not an independent type of service, but a way of delivering part of the content or process to the user. Most public services are hybrids and contain both digital and non-digital components, such as human labour, physical presence or administrative operations. Therefore, the ownership and organisation of both the service as a whole and its digital component can be decided separately. See also Chapter 1.3.6 and "ANNEX 3 Issue of the state's core function"

5 My digital service is unique and therefore there is no reason for the private sector to provide it.

Many services and digital services are actually not unique in their essence. While there may be specific differences in certain solutions, their main functions often overlap with solutions that already exist. Similar digital services can be found in the private sector – e.g. the internal tools of large corporations are often similar to those used in the public sector – as well as in other public authorities or other countries. This is why the private sector is often interested in developing such digital solutions: if the solution is universal enough, its target group is not limited to a single customer and can have a wide international or cross-sectoral user base. See also Chapters 1.1.2, 1.1.4 and 1.2.

6 If the digital service is provided by the private sector, the state has no control over it.

It is true that, in principle, the owner of the digital service has the right to decide on the provision of the service. However, the state can establish clear conditions that regulate how and on what basis digital services are provided. For example, it can demand that the code be deposited with a notary, demand longer notice periods for the termination of digital services and compliance with certain technical, quality and security requirements, and ensure supervision by the state. Such measures help to significantly reduce the impact and likelihood of potential risks by bringing them to acceptable levels. It's important to understand that unexpected things can also occur with digital services managed by the state itself – thus, the solutions of the private sector are not riskier in essence, but simply require good management. See Chapter 1.3.

7 The private sector is not familiar with the specificities of the public sector and is unable to take them into account

It is widely believed that only people who work in the public sector have an adequate understanding of public processes, the legal framework and administrative practices. In reality, many private sector partners have long-term experience working with the public sector, and in the case of good cooperation, this knowledge can be deepened by working together and setting clear expectations.

8 If the state is not the only customer, the digital services cannot be sufficiently influenced.

It is often thought that if a digital service is universal and intended for a wider market, the state loses the opportunity to impose its needs. In reality, a diverse customer base often means better service development, faster response times and lower prices. Instead of demanding adaptations that only meet the needs of the state, the state should look for smart ways to adapt its processes and requirements to fit a high-quality standard solution. This helps ensure effective cooperation and avoids the need for costly special solutions. See also Chapters 1.2.1 and 1.2.2.

9 When a digital service has many customers, the needs of the state take a back seat.

People think that if a service provider serves a large number of customers, the special needs of the state will not be given enough attention. In reality, a diverse user base can be an advantage: it speeds up development cycles, highlights problems faster and enables the deployment of solutions that an individual customer might not think of on their own. In addition, for a private sector service provider, maintaining customer satisfaction and reputation is critical for business – this also applies in the case of the state as a customer. Good cooperation, clear expectations and transparent feedback help ensure that the state's needs are actually taken into account.

10 When the state communicates with the private sector to look into existing solutions, there is a risk of a breach of law or corruption.

It is a common misconception that simply communicating with the private sector before a procurement is launched can be illegal or create a risk of corruption. In reality, market research or consultation carried out on equal terms is perfect- ly acceptable and advisable, as long as it is trans- parent and documented. Gathering information from market players helps the state make more informed decisions, map existing solutions and avoid duplication. It is important to follow the principles of equal treatment and transparency, not to avoid contact – informed and well-managed communication reduces risks instead of increas-ing them. See also Chapter 1.2.3.

11 Today's rules and organisation of work do not allow outsourcing digital services to the private sector.

People often think that if the current legal framework or organisation of work do not allow outsourcing digital services to the private sector, then it is completely ruled out. In reality, all rules, processes and frameworks are designed by people themselves and therefore can be changed with time – including legislation. Often, the problem is not that something cannot be changed, but whether the person who wants to make the change has the necessary power. For example, if outsourcing a digital service requires changing a law or regulation, this is not a technical decision that the product owner of an IT centre can implement. The product owner has no leverage in changing the system or the regulatory framework – and that is not their role either. The responsibility for such strategic decisions rests with the service owner as the policy maker. This is why the right parties must be involved and decisions must be made cooperatively when systemic changes are planned. See also Chapter 1.3.6.

Lisa 3

Issue of the state's core function

Guide for the public sector in planning the development of digital services

Although from the perspective of expenses, efficiency and public interest, it would be reasonable for the state not to provide a service itself if there is a more suitable provider on the market, it must be kept in mind that a full transfer of the state's functions to the private sector is not allowed.

Based on the Constitution, the state's functions can be divided into three:

1. Functions performed by specific authorities assigned to the state (Riigikogu, President, Government of the Republic, Chancellor of Justice, National Audit Office, Eesti Pank).
2. Functions that the state is obliged to perform, but the specific authority that performs them has not been defined.
3. Functions assigned to the state indirectly.

According to Supreme Court Judgment No 3-1-1-86-07 of 16.05.2008, the state may not delegate to private legal entities any of the functions that are among the core functions of the state, such as penal power, administration of justice and legislation. However, the state may involve the private sector in the performance of certain administrative functions if the provisions delegating the authority for this are provided for by law.

The delegation of a public service means that the state delegates the task of providing a service to a private organisation, but remains ultimately responsible for the service and must ensure supervision. If it is a core function of the state, an administrative contract can only be concluded if this is clearly permitted by law. If the law does not permit this, an administrative contract may not be concluded.

Pursuant to § 3 (1) of the Administrative Cooperation Act, the authorisation may come from the law, an administrative act issued on the basis of the law or an administrative contract entered into under the conditions and pursuant to the procedure provided for in the Administrative Cooperation Act. Subsection (4) of the same provision stipulates that upon the granting of authorisation for performance of administrative duties, a civil law contract may be entered into unless only entry into an administrative contract is provided by law, the contract regulates the rights or obligations of persons using public services or other third persons, the state or a local government is released from its duties, or the authority to exercise executive power is used upon performance of the duties. If a contract does not clearly reflect the intention of the parties to enter into a civil law contract, it is presumed to be an administrative contract.

All in all, the state may outsource services (including digital services) to private entities that support the core functions of state authority, but do not transfer the right to make decisions or exercise power. For example, it is not permitted to delegate the protection of fundamental rights, legislative drafting, the activities of courts, the decision-making on key issues of state governance or the exercise of public authority. At the same time, even in the case of a core function, the private sector can be involved in activities that support, assist and prepare the core function. This means that where the development or provision of services does not involve the exercise of power, there is no obstacle to private sector involvement. The state remains the owner of the service, but the developer, for example, is found from the private sector.

Annex 4

Worksheet for preparations: Current description of the digital service

Guide for the public sector in planning the development of digital services

Name of the digital service:

The problem solved by the digital service:

Brief description of the content of the digital

Users of digital services and their number (per month/year):

Current cost of provision of the (digital) service (per year):

Main risks in providing the digital service: